SOLUCION DE DOS ESTUDIOS DE CASO BAJO EL USO DE TECNOLOGIA CISCO

DIPLOMADO DE PROFUNDIZACION CISCO CCNA PARA OPTAR AL TITULO DE INGENIERO DE SISTEMAS

CAMILO ANDRES RAMIREZ RIVEROS

ASESOR: JUAN CARLOS VESGA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA (ECBTI)
DIPLOMADO DE CISCO, INGENIERÍA DE SISTEMAS
BOGOTÁ, COLOMBIA MAYO, 2020

Nota de aceptación

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

CONTENIDO

pag

LISTA DE TABLAS

pag

LISTA DE FIGURAS

pag

INTRODUCCION

Por medio de esta prueba de habilidades se pretende realizar dos ejercicios de Redes utilizando el simulador de Packer Tracer para configurar las redes de empresas que lo requieren donde se tendrán en cuenta conocimientos de rutas, direccionamientos, direcciones ipv6 y ipv4, host dinámicos, traducción de direcciones de red dinámicas y estáticas, listas de control de acceso, protocolo de tiempo de red, el uso de OSPF como protocolo de enrutamiento, encapsulamiento PPP y su autenticación entre otros para configurar y poner andar estas redes.

Para dar comienzo a la presente unidad, se desarrollarán de manera sistemática una serie de ejercicios (laboratorios) detallando en pormenor los pasos, aplicaciones y comandos que darán origen a preguntas con el ánimo de reforzar el procedimiento y afianzar la labor realizada. Por medio de líneas de código se programa las sentencias de ACL, que emiten los routers para poder enviar y recibir paquetes.

El ejercicio que se realizara es para activar y desactivar las ACL's para incorporar dinámicas a las unidades conectadas, esto es en fin de realizar el procedimiento de los comandos específicos.

El análisis de IPv6 ACL permitirá establecer un protocolo de la programación del enrutamiento, cumpliendo con lo requerido, ya sea desde IPv4 a IPV6 respectivamente.
También se realizará configuración DHCPv6 en diferentes estados para verificar como los hosts funcionan la información y que mensajes muestra en los routers, esto es importante para establecer las condiciones que se necesitan en redes domesticas mediante IDT y DCHP para identificar cualquier ID que se conecte a las redes establecidas

También se programará las direcciones de red (NAT), el motivo principal para usar NAT es reducir el número de direcciones IP públicas que usa una organización, ya que la cantidad de direcciones IPv4 públicas disponibles es limitada. Se analizará el protocolo que proporciona seis direcciones IP públicas a la empresa.

Todo esto se podrá definir en este informe, desglosado de una manera que se pueda mostrar lo ya mencionado.

OBJETIVOS

OBJETIVO GENERAL

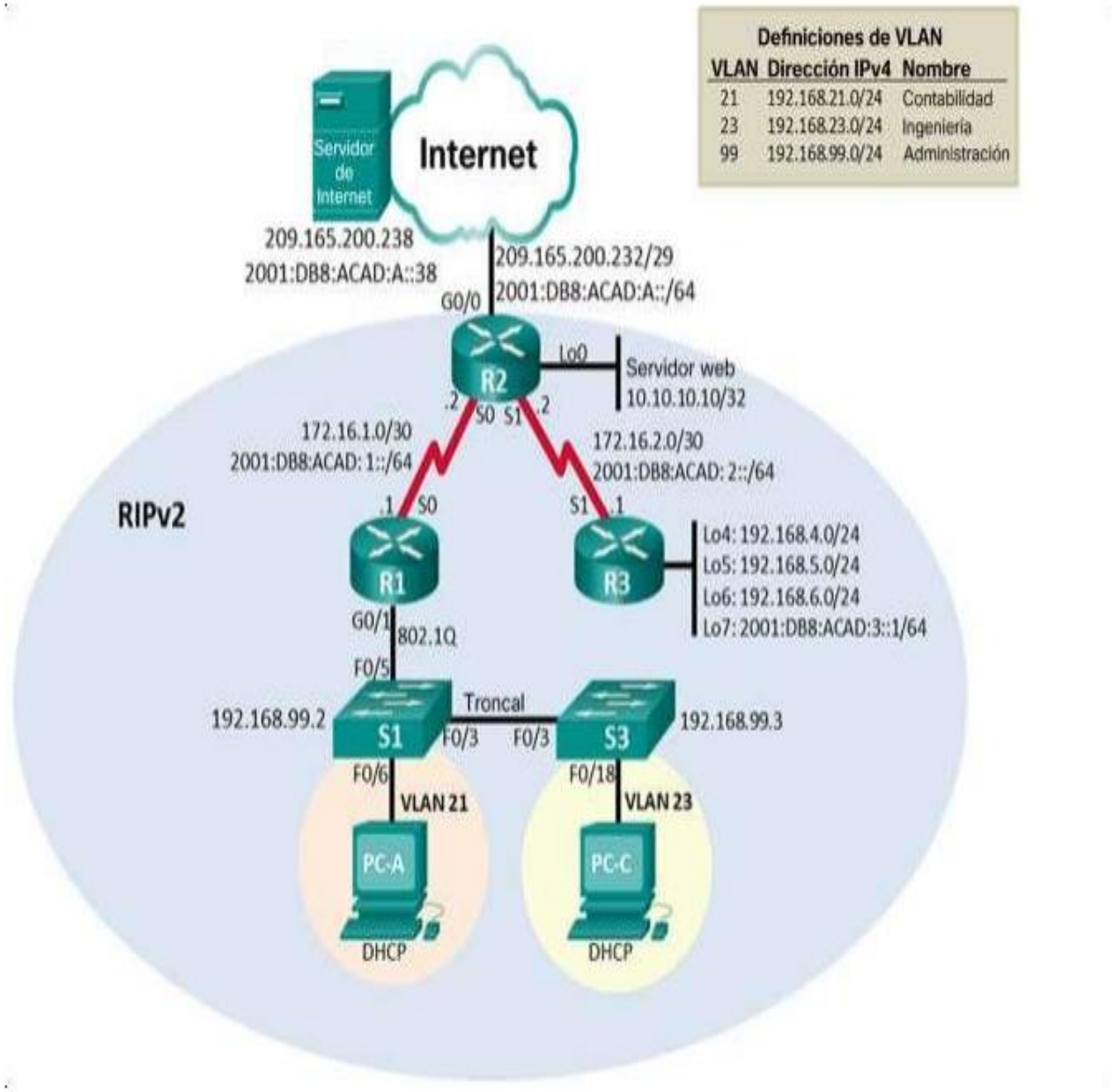
- Aprender y conocer habilidades en el estudio de enrutamiento en soluciones de red, realizando ejercicios planteados en el trabajo del Diplomado de Profundización CISCO.

OBJETIVOS ESPECIFICOS

- Incluir y reconocer las competencias designados para esta unidad.
- Aprender como estructurar y características principales de las redes.convergentes.
- Demostrar todas las posibles soluciones.
- Aplicar la configuración básica para un Switch y un Router.
- Dar a conocer los protocolos de seguridad usados en los Switch.
- Configurar y aplicar una ACL nombrada estándar.
- Aprender a configurar redes y los parámetros de los dispositivos.

ESCENARIO: Se debe configurar una red pequeña para que admita conectividad IPv4 e IPv6, seguridad de switches, routing entre VLAN, el protocolo de routing dinámico RIPv2, el protocolo de configuración de hosts dinámicos (DHCP), la traducción de direcciones de red dinámicas y estáticas (NAT), listas de control de acceso (ACL) y el protocolo de tiempo de red (NTP) servidor/cliente. Durante la evaluación, probará y registrará la red mediante los comandos comunes de CLI.

TOPOLOGIA



PARTE 1: Inicializar dispositivos

PASO 1: Inicializar y volver a cargar los routers y los switches

Elimine las configuraciones de inicio y vuelva a cargar los dispositivos. Antes de continuar, solicite al instructor que verifique la inicialización de los dispositivos.

Iniciar y volver a cargar el router

Para este primer ejercicio se de iniciar con acceder al router mediante el puerto de consola y habilite el modo EXEC privilegiado, después se debe escribir el comando erase startup-config para eliminar para eliminar el archivo de configuración de inicio de la NVRAM. Después se emite el comando o reload para eliminar una configuración antigua de la memoria. Cuando reciba el mensaje Proceed with reload. Una vez que se vuelve a cargar el router, se le solicita introducir el diálogo de configuración inicial. Escriba no y presione Enter. Se le solicita finalizar la instalación automática, se escribe yes y, luego, se presiona Enter.

Iniciar y volver a cargar el switch**.**

Se accede al switch mediante el puerto de consola e ingrese al modo EXEC privilegiado. Se utiliza el comando show flash para determinar si se crearon VLAN en el switch. Se utiliza el comando erase startup-config para eliminar el archivo de configuración de inicio de la NVRAM. Se solicitará que confirme la eliminación del archivo de configuración. Presione Enter para confirmar que desea borrar este archivo. Después se emite el comando o reload para eliminar una configuración antigua de la memoria. Cuando reciba el mensaje Proceed with reload. Una vez que se vuelve a cargar el router, se le solicita introducir el diálogo de configuración inicial. Escriba no y presione Enter. Se le solicita finalizar la instalación automática, se escribe yes y, luego, se presiona Enter.

Tarea	Comando de IOS
Eliminar el archivo startup-config de todos los routers	Router#erase startup-config
Volver a cargar todos los routers	Router#reload
Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior	Switch#erase startup-config Switch#delete flash:vlan.dat
Volver a cargar ambos switches	Switch#reload

Tabla 1. Carga de routers y switches

PARTE 2: Configurar los parámetros básicos de los dispositivos

PASO 1: Configurar la computadora de Internet

Las tareas de configuración del servidor de Internet incluyen lo siguiente (para obtener información de las direcciones IP, consulte la topología):

Se configura la topología de la red y los parámetros básicos, con direcciones IP de la interfaz, en el acceso de los dispositivos y contraseñas. Se Configura la dirección IP, la máscara de subred y los parámetros del gateway predeterminado

Elemento o tarea de configuración	Especificación
Dirección IPv4	209.165.200.238
Máscara de subred para IPv4	255.255.255.248
Gateway predeterminado	209.165.200.225
Dirección IPv6/subred	2001:db8:acad:a::38/64
Gateway predeterminado IPv6	2001:DB8:ACAD:A::1

Tabla 2. Configuración de dispositivos

Nota: Quizá sea necesario deshabilitar el firewall de las computadoras para que los pings se realicen correctamente en partes posteriores de esta práctica de laboratorio.

PASO 2: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Se desactiva la búsqueda DNS con el comando no ip domain-lookup para que sea rápida y no sea insensible, después se nombra el router como R1, después se crea una contraseña de acceso de exclusivo privilegiado llamada class y contraseña de acceso a la consola cual es cisco y la contraseña de Telner la cual es cisco también. Después se cifran las contraseñas de texto no cifrado por medio del código service password-encryption, y después se configura un mensaje de acceso no autorizado con un banner motd. Por Ultimo se crea la interfaz S0/0/0 para la dirección IPV6 y IPV4 para conocer la información de las direcciones cuales son 172.16.1.1 con su máscara 255.255.255.252 para la IPV4 y 2001:DB8:ACAD:1::/64 para la IPV6 y se establece una frecuencia de reloj en 128000 y se activa la interfaz y se configura las rutas predeterminadas para la IPV4 y IPV6 cuales son 0.0.0.0 0.0.0.0 y ::/0 s0/0/0 respectivamente.

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router(config)#no ip domain-lookup
Nombre del router	R1
Contraseña de exec privilegiad cifrada	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no cifrado	R1(config)#enable secret class R1(config)#line console 0 R1(config-line)#password cisco R1(config-line)#login R1(config-line)#exit R1(config)#line vty 0 4 R1(config-line)#password cisco R1(config-line)#login R1(config-line)#exit R1(config)#service password-encryption
Mensaje MOTD	R1(config)#banner motd #Se prohbe el acceso no autorizado!#
Interfaz S0/0/0	Int s0/0/0 R1(config-if)#ip address 172.16.1.1 255.255.255.252 R1(config-if)#ipv6 address 2001:DB8:ACAD:1::/64 R1(config-if)#clock rate 128000 R1(config-if)#no shutdown
Rutas predeterminadas	R1(config)#ip route 0.0.0.0 0.0.0.0 s0/0/0 R1(config)#ipv6 route ::/0 s0/0/0

Tabla 3. Configuración router 1

Nota: Todavía no configure G0/1.

PASO 3: Configurar R2

La configuración del R2 incluye las siguientes tareas:

Se desactiva la búsqueda DNS con el comando no ip domain-lookup para que sea rápida y no sea insensible, después se nombra el router como R2, después se crea una contraseña de acceso de excusión privilegiado llamada class y contraseña de acceso a la consola cual es cisco y la contraseña de Telner la cual es cisco también. Después se cifran las contraseñas de texto no cifrado por medio del código service password-encryption. Por Ultimo se crea la interfaz S0/0/0 para la dirección IPV6 y IPV4 para conocer la información de las direcciones cuales son 172.16.1.2 con su

máscara 255.255.255.252 para la IPV4 y 2001:DB8:ACAD:2::/64 para la IPV6 y se establece una frecuencia de reloj en 128000. Después se configura la interface S0/0/1 con sus direcciones IPV4 y IPV6 respectivamente, las cuales son 172.16.2.2 255.255.255.252 y 2001:DB8:ACAD:2::1/64 y con su frecuencia de reloj en 128000. Para la interface G0/0 se establece la dirección IPV4 y se utiliza la siguiente dirección disponible en la subred 209.165.200.233 255.255.255.248 para la IPV6 se utiliza 2001:DB8:ACAD:A::2/64. Después de eso se configura la interfaz loopback 0 y se establecen las direcciones para la IPV4, siendo 10.10.10.10 255.255.255.0 y se configuran las rutas predeterminadas para IPV4 y IPV6 respectivamente 0.0.0.0 0.0.0.0 go/0,:/0 g0/0.

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	Router(config)#no ip domain-lookup
Nombre del router	R2
Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no cifrado	R2(config)#enable secret class R2(config)#line console 0 R2(config-line)#password cisco R2(config-line)#login R2(config-line)#exit R2(config)#line vty 0 4 R2(config-line)#password cisco R2(config-line)#login R2(config-line)#exit R2(config)#service password-encryption
Habilitar el servidor HTTP	router(config)# ip http server
Interfaz S0/0/0	R2(config-if)#ip address 172.16.1.2 255.255.255.252 R2(config-if)#no shutdown R2(config-if)#ipv6 address 2001:DB8:ACAD:1::2/64 R2(config-if)#no shutdown
Interfaz S0/0/1	R2(config-if)#ip address 172.16.2.2 255.255.255.252 R2(config-if)#clock rate 128000 R2(config-if)#no shutdown R2(config)#interface s0/0/1 R2(config-if)#ipv6 address 2001:DB8:ACAD:2::1/64 R2(config-if)#clock rate 128000 R2(config-if)#no shutdown

Interfaz G0/0 (simulación de Internet)	R2(config)#interface g0/0 R2(config-if)#ip address 209.165.200.233 255.255.255.248 R2(config-if)#no shutdown R2(config-if)#ipv6 address 2001:DB8:ACAD:A::2/64 R2(config-if)#no shutdown
Interfaz loopback 0 (servidor web simulado)	R2(config)#interface loopback 0 R2(config-if)#ip address 10.10.10.10 255.255.255.0 R2(config-if)#no shutdown R2(config)#ip route 0.0.0.0 0.0.0.0 g0/0 R2(config)#ipv6 route ::/0 g0/0
Rutas predeterminadas	R2(config)#ip route 0.0.0.0 0.0.0.0 g0/0 R2(config)#ipv6 route ::/0 g0/0

Tabla 4. Configuración router 2

PASO 4: Configurar R3

La configuración del R3 incluye las siguientes tareas:

Se desactiva la búsqueda DNS con el comando no ip domain-lookup para que sea rápida y no sea insensible, después se nombra el router como R3, después se crea una contraseña de acceso de exclusivo privilegiado llamada class y contraseña de acceso a la consola cual es cisco y la contraseña de Telner la cual es cisco también. Después se cifran las contraseñas de texto no cifrado por medio del código service password-encryption, y después se configura un mensaje de acceso no autorizado con un banner motd. Por Ultimo se crea la interfaz S0/0/1 para la dirección IPV4 para conocer la información de la dirección cual es 172.16.2.1 con su máscara 255.255.255. Después de eso se configura la interfaz loopback 4 y se establecen las dirección para la IPV4, siendo 192.168.4.1 255.255.255.0, también para la interfaz loopback 5 con dirección IPV4 192.168.5.1 255.255.255.0 y para el looback 6, dirección IPV4 192.168.6.1 255.255.255.0 y or ultimo la interface loopback 7 con IPV4 2001:DB8:ACAD:3::1/64 y se establecen las direcciones para la IPV4, siendo 10.10.10.10 255.255.255.0 y se configuran las rutas predeterminadas para IPV4 y IPV6 respectivamente 0.0.0.0 0.0.0.0, ::/0

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router(config)#no ip domain-lookup
Nombre del router	R3
Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no cifrado	R3(config)#enable secret class R3(config)#line console 0 R3(config-line)#password cisco R3(config-line)#login R3(config-line)#exit R3(config)#line vty 0 4 R3(config-line)#password cisco R3(config-line)#login R3(config-line)#exit R3(config)#service password-encryption
Mensaje MOTD	R3(config)#banner motd #Se prohbe el acceso no autorizado! #.
Interfaz S0/0/1	R3(config-if)#ip address 172.16.2.1 255.255.255.252 R3(config-if)#no shutdown
Interfaz loopback 4	R3(config)#interface loopback 4 R3(config-if)#ip address 192.168.4.1 255.255.255.0
Interfaz loopback 5	R3(config)#interface loopback 5 R3(config-if)#ip address 192.168.5.1 255.255.255.0
Interfaz loopback 6	R3(config)#interface loopback 6 R3(config-if)#ip address 192.168.6.1 255.255.255.0
Interfaz loopback 7	R3(config)#interface loopback 7 R3(config-if)#ipv6 address 2001:DB8:ACAD:3::1/64
Rutas predeterminadas	R3(config-if)#ip route 0.0.0.0 0.0.0.0 R3(config-if)#ipv6 route ::/0

Tabla 5. Configuración router 3

PASO 5: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Se desactiva la búsqueda DNS con el comando no ip domain-lookup para que sea rápida y no sea insensible, después se nombra el router como S1, después se crea una contraseña de acceso de exclusivo privilegiado llamada class y contraseña de acceso a la consola cual es cisco y la contraseña de Telner la cual es cisco también. Después se cifran las contraseñas de texto no cifrado por medio del código service password-encryption, y después se configura un mensaje de acceso no autorizado con un banner motd.

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Switch(config)#no ip domain-lookup
Nombre del switch	S1
Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no cifrado	S1(config)#enable secret class S1(config)#line console 0 S1(config-line)#password cisco S1(config-line)#login S1(config-line)#line vty 0 4 S1(config-line)#password cisco S1(config-line)#login S1(config-line)#service password-encryption
Mensaje MOTD	S1(config)#banner motd #Se prohbe el acceso no autorizado!#

Tabla 5. Configuración switch 1

PASO 6: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Se desactiva la búsqueda DNS con el comando no ip domain-lookup para que sea rápida y no sea insensible, después se nombra el router como S1, después se crea una contraseña de acceso de exclusivo privilegiado llamada class y contraseña de acceso a la consola cual es cisco y la contraseña de Telner la cual es cisco también. Después se cifran las contraseñas de texto no cifrado por medio del código service password-encryption, y después se configura un mensaje de acceso no autorizado con un banner motd.

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Switch(config)#no ip domain-lookup
Nombre del switch	S3
Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no cifrado	S3(config)#enable secret class S3(config)#line console 0 S3(config-line)#password cisco S3(config-line)#login S3(config-line)#line vty 0 4 S3(config-line)#password cisco S3(config-line)#login S3(config-line)#service password-encryption
Mensaje MOTD	S3(config)#banner motd #Se prohbe el acceso no autorizado!#

Tabla 6. Configuración Switch 3

PASO 7: Verificar la conectividad de la red

Utilice el comando ping para probar la conectividad entre los dispositivos de red.

Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

Se realiza los pings de los routers R1 a R2, de R2 a R3 y de la PC a él Gateway. Para el ping de R1 a R2 se utiliza la dirección de IP 172.16.1.2 y del router R2 al 3 se utiliza la dirección 172.16.2.1, para el ping de PC al Gateway se utiliza la dirección

Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/0/0	172.16.1.2	Successfull
R2	R3, S0/0/1	172.16.2.1	Successfull
PC de Internet	Gateway predeterminado	209.165.200.233	Successfull

Tabla 7. Conectividad de red

PING, desde R1 a R2, (172.16.1.2)

Se hace un Ping para confirmar la conexión entre el router R1 y el router R2 con el ip address 172.16.1.2 y se demuestra exitoso.

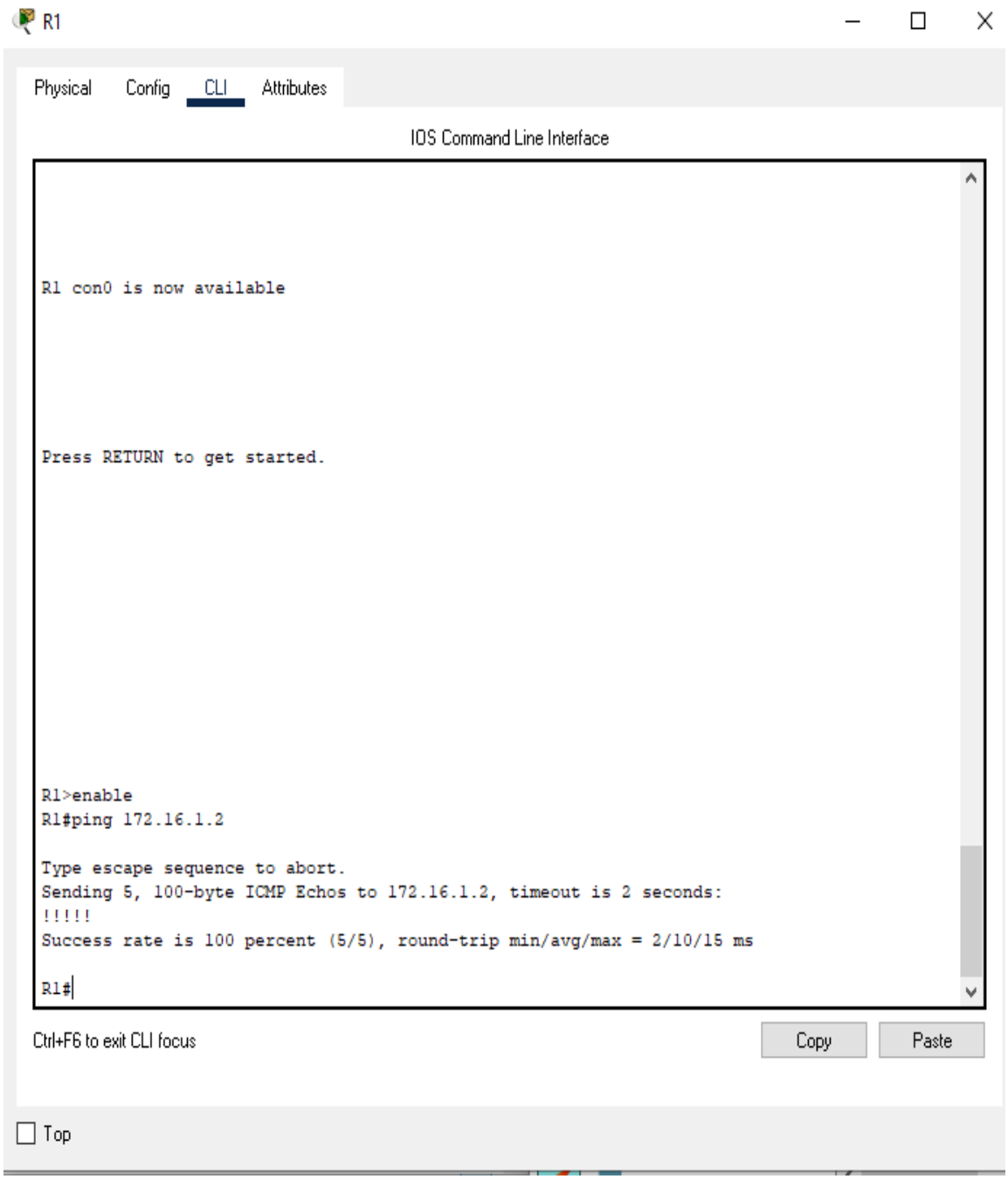


Figura 1. Ping R1 a R2. Ingeniería de sistemas

PING, desde R2 a R3, (172.16.2.1)

Se hace un Ping para confirmar la conexión entre el router R2 y el router R3 con el ip address 172.16.2.1 y se demuestra exitoso.

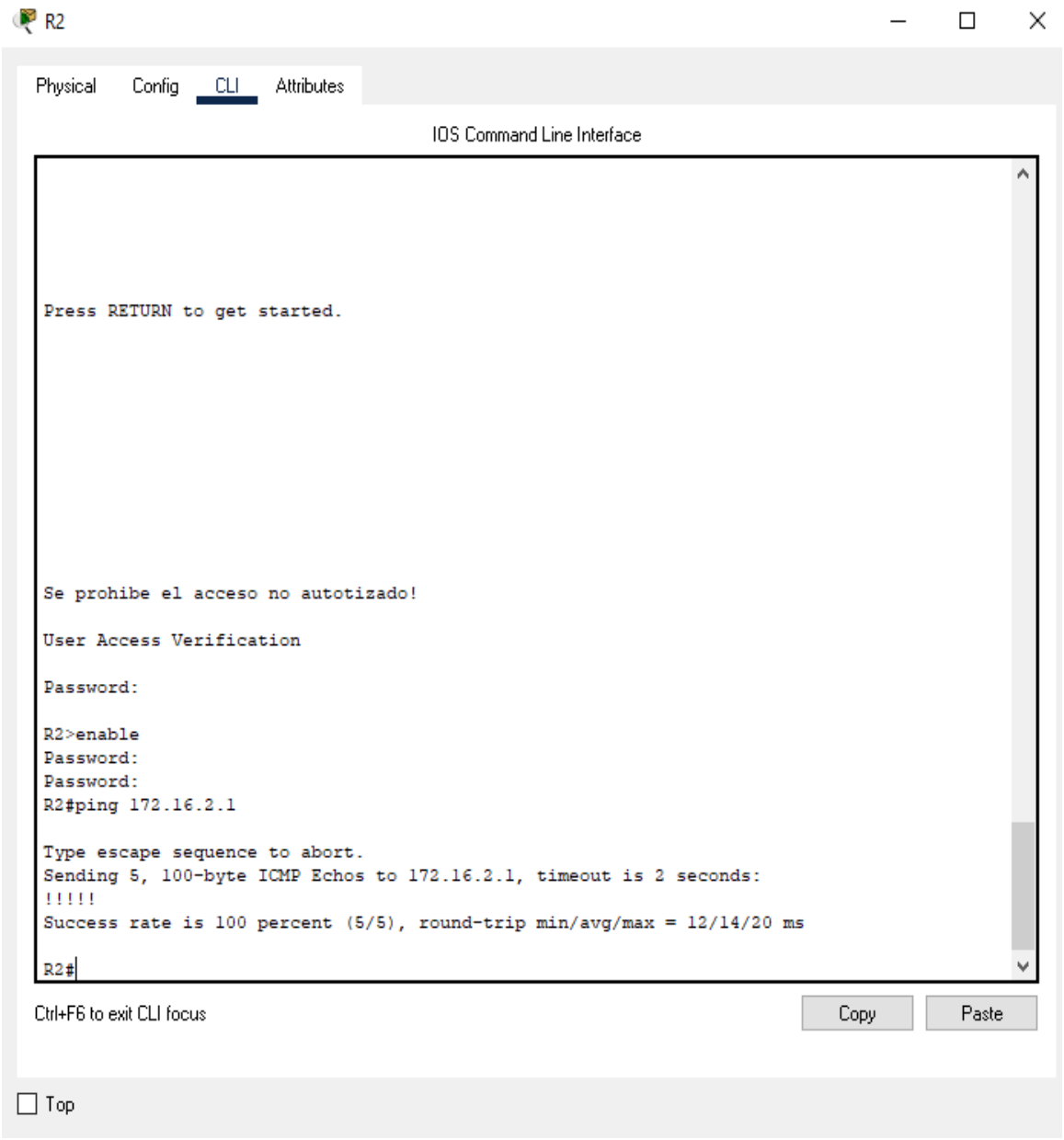


Figura 2. Ping R2 a R3. Ingeniería de sistemas

PING, desde Pc de Internet a gateway, (10.10.10.10)

Se hace un Ping para confirmar la conexión entre el router desde el PC de Internet al gateway con el ip address 10.10.10.10 y se demuestra exitoso.

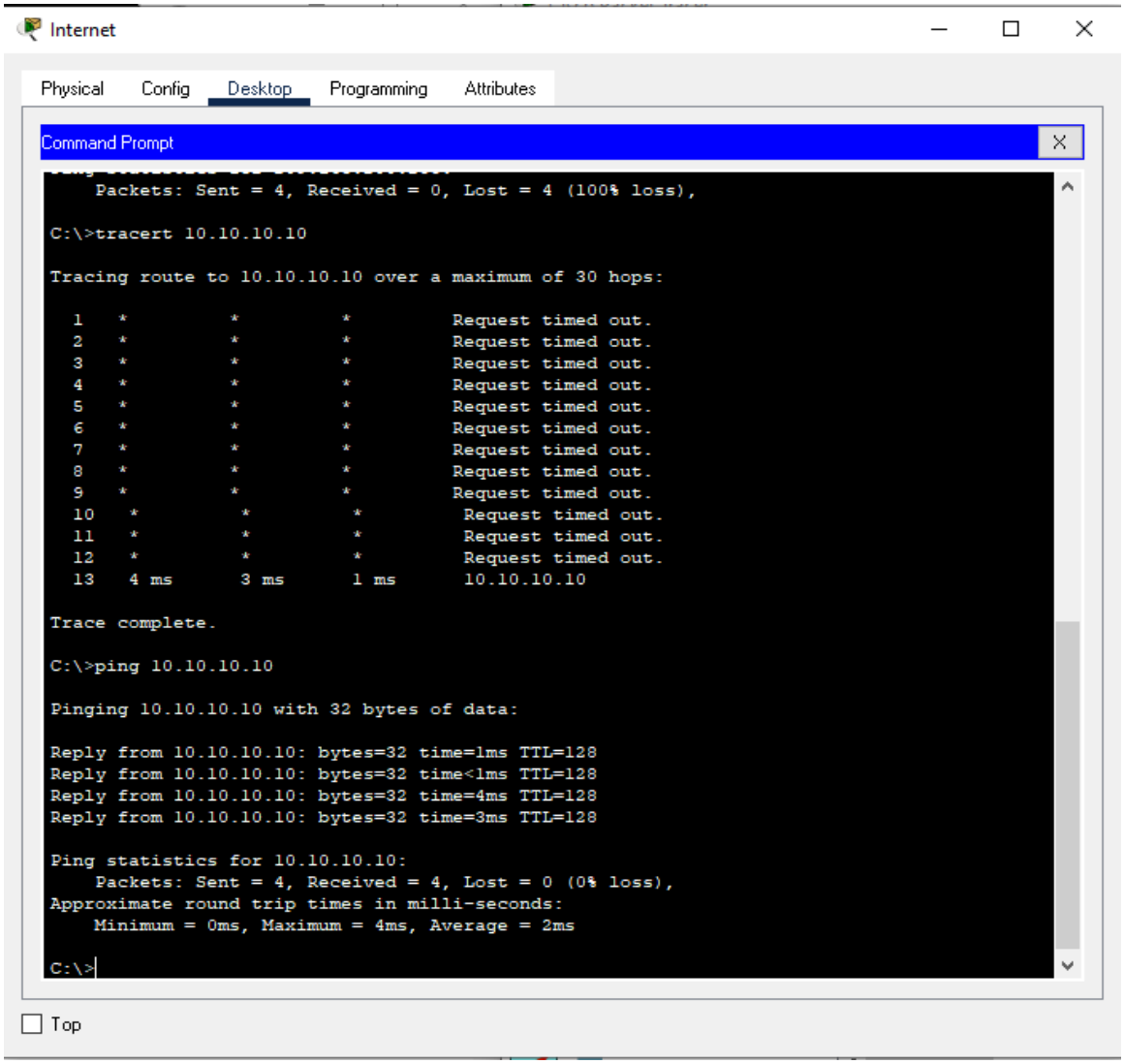


Figura 3. Ping de PC a Gateway. Ingeniería de sistemas

Nota: Quizá sea necesario deshabilitar el firewall de las computadoras para que los pings se realicen correctamente.

PARTE 3: Configurar la seguridad del switch, las VLAN y el routing entre VLAN

PASO 1: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Para configurar el switch S1 con la topología VLAN y se nombra cada una según los cargos en este caso es Administración, Contabilidad e Ingeniería, después de esto se le asignan a el cargo de Administración la dirección IPv4 que en este caso es 192.168.99.2 255.255.255.0 ya teniendo esto se asigna el Gateway predeterminado que es 192.168.99.1 en este caso se utilizó la dirección IPV4 de la subred. Se busca forzar el enlace troncal en la interface f0/3 donde se utiliza la red VLAN 1 como Vlan nativa lo mismo se hace para forzar el enlace troncal en la interfaz F0/5 donde se utiliza la red VLAN 1 como VLAN nativa, después se configura el resto de los puertos como puertos de acceso al utilizar el comando range f0/1, f0/2, f0/4, f0/7-24, g0/1-2. Lo siguiente se asigna la interfaz F0/6 a la VLAN 21 y por último se apaga todos los puertos que no se usan con el comando shutdown.

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	S1(config)#vlan 99} S1(config-vlan)#name Administracion S1(config-vlan)#vlan 21 S1(config-vlan)#name Contabilidad S1(config-vlan)#vlan 23 S1(config-vlan)#name Ingenieria
Asignar la dirección IP de administración.	S1(config)#interface vlan 99 S1(config-if)#ip address 192.168.99.2 255.255.255.0
Asignar el gateway predeterminado	S1(config)#ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	S1(config)#interface f0/3 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1
Forzar el enlace troncal en la interfaz F0/5	S1(config)#interface f0/5 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1
Configurar el resto de los puertos como puertos de acceso	S1(config-if)#interface range f0/1, f0/2, f0/4, f0/7-24, g0/1-2
Asignar F0/6 a la VLAN 21	S1(config)#interface f0/6 S1(config-if)#switchport mode access S1(config-if)#switchport access vlan 21
Apagar todos los puertos sin usar	S1(config-if-range)#shutdown

Tabla 8. Configuración VLAN switch 1

PASO 2: Configurar el S3

S3 configuración del S3 incluye las siguientes tareas:

Para configurar el switch S3 con la topología VLAN y se nombra cada una según los cargos en este caso es Administración, Contabilidad e Ingeniería, después de esto se le asignan a el cargo de Administración la dirección IPv4 que en este caso es 192.168.99.3 255.255.255.0 ya teniendo esto se asigna el Gateway predeterminado que es192.168.99.1 en este caso se utilizó la dirección IPV4 de la subred. Se busca forzar el enlace troncal en la interface f0/3 donde se utiliza la red VLAN 1 como Vlan nativa lo mismo se hace para forzar el enlace troncal en la interfaz F0/5 donde se utiliza la red VLAN 1 como VLAN nativa, después se configura el resto de los puertos como puertos de acceso al utilizar el comando range f0/1-2, f0/4-17, f0/19-24, g0/1-2. Lo siguiente se asigna la interfaz F0/6 a la VLAN 21 y por último se apaga todos los puertos que no se usan con el comando shutdown.

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	S3(config)#vlan 21 S3(config-vlan)#name Contabilidad 23 S3(config-vlan)#name Ingenieria S3(config-vlan)#vlan 99 S3(config-vlan)#name Administracion
Asignar la dirección IP de administración	S3(config)#interface vlan 99 S3(config-if)#ip address 192.168.99.3 255.255.255.0
Asignar el gateway predeterminado.	Ip default-gateway 192.168.99.3 255.255.255.0
Forzar el enlace troncal en la interfaz F0/3	S3(config)#interface f0/3 S3(config-if)#switchport mode trunk S3(config-if)#switchport trunk native vlan 1
Configurar el resto de los puertos como puertos de acceso	S3(config)#interface range f0/1-2, f0/4-17, f0/19-24, g0/1-2
Asignar F0/18 a la VLAN 21	S3(config)#interface f0/8 S3(config-if)#no shutdown S3(config-if)#switchport mode Access S3(config-if)#switchport access vlan 23
Apagar todos los puertos sin usar	shutdown

Tabla 9. Configuración VLAN switch 3

PASO 3: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Se continua con la configuración del router R1. Se configura la subinterfaz 802.1Q .21 en G0/1 con la descripción LAN_Contabilidad y se asigna la VLAN 21 como también la primera dirección disponible a esta interfaz que es 192.168.21.2 255.255.255.0. También se hace esto para la subinterfaz 802.1Q .23 en G0/1 con la descripción LAN_Ingenieria y se le asigna la VLAN 23 con la dirección 192.168.23.2 255.255.255.0, esto mismo para la subinterfaz 802.1Q .99 en G0/1 con descripción la LAN_Ingenieria asignándole la VLAN 23 con dirección 192.168.99.1 255.255.255.0, por último, se activa la interfaz G0/1.

Elemento o tarea de configuración	Especificación
Configurar la subinterfaz 802.1Q .21 en G0/1	R1(config)#interface g0/1.21 R1(config-subif)#description LAN_Contabilidad R1(config-subif)#encapsulation dot1q 21 R1(config-subif)#ip address 192.168.21.2 255.255.255.0
Configurar la subinterfaz 802.1Q .23 en G0/1	R1(config)#interface g0/1.23 R1(config-subif)#description LAN_Ingenieria R1(config-subif)#encapsulation dot1q 23 R1(config-subif)#ip address 192.168.23.2 255.255.255.0
Configurar la subinterfaz 802.1Q .99 en G0/1	R1(config)#interface g0/1.99 R1(config-subif)#description LAN_Administracion R1(config-subif)#encapsulation dot1q 99 R1(config-subif)#ip address 192.168.99.1 255.255.255.0
Activar la interfaz G0/1	R1(config)#interface g0/1

Tabla 10. Configuración Subinterfaz router 1

PASO 4: Verificar la conectividad de la red

Utilice el comando **ping** para probar la conectividad entre los switches y el R1.

Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red.

Se realiza los pings de los routers S1 a R1 con dirección 192.168.99.1 al VLAN 99,

de S3 a R1con dirección 192.168.99.1 a VLAN 99, de S1 a R1 con dirección 192.168.21.1 a VLAN 21, de S3 a R1 con dirección 192.168.23.1 a VLAN 23.

Desde	A	Dirección IP	Resultados de ping
S1	R1, dirección VLAN 99	192.168.99.1	Successfull
S3	R1, dirección VLAN 99	192.168.99.1	Successfull
S1	R1, dirección VLAN 21	192.168.21.1	Successfull
S3	R1, dirección VLAN 23	192.168.23.1	Successfull

Tabla 11. Verificación de Conectividad de red

S1 a R1 con, (192.168.99.1) y de S1 a R1 con, (192.168.21.1)

Se hace un Ping del switch S1 al router R1 con la configuracion de VLAN 99 y una dirección de IP 192.168.99.1, también se hace Ping del Switch S1 al router R1 con la configuración de VLAN 21 y una dirección de IP 192.168.21.1, con el fin de verificar su conectividad y se demuestra exitoso.

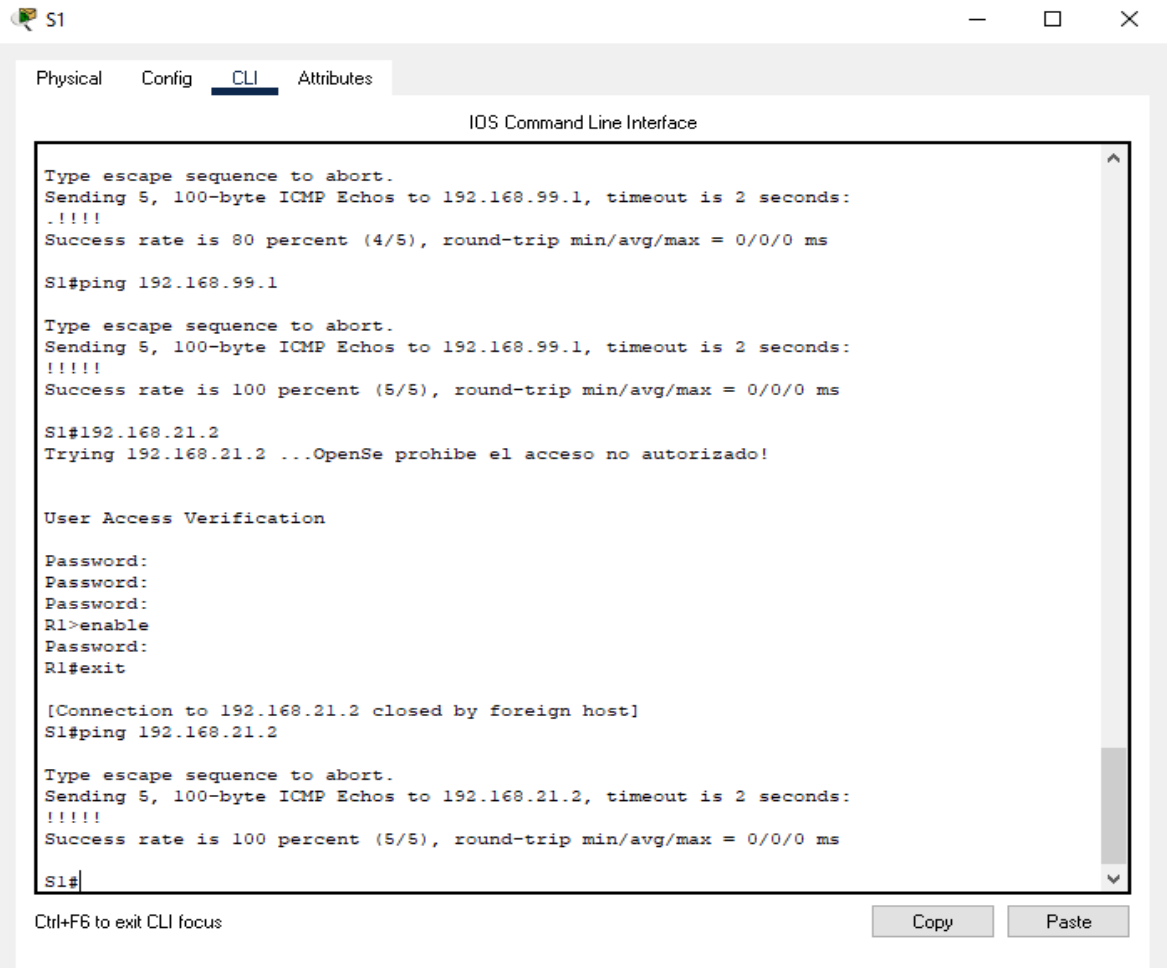


Figura 4. Ping de S1 a R1 con VLAN 99 y VLAN 21. Ingeniería de sistemas

S3

Se hace un Ping del switch S3 al router R1 con la configuracion de VLAN 99 y una dirección de IP 192.168.99.1, también se hace Ping del Switch S3 al router R1 con la configuración de VLAN 21 y una dirección de IP 192.168.23.1, con el fin de verificar su conectividad y se demuestra exitoso.

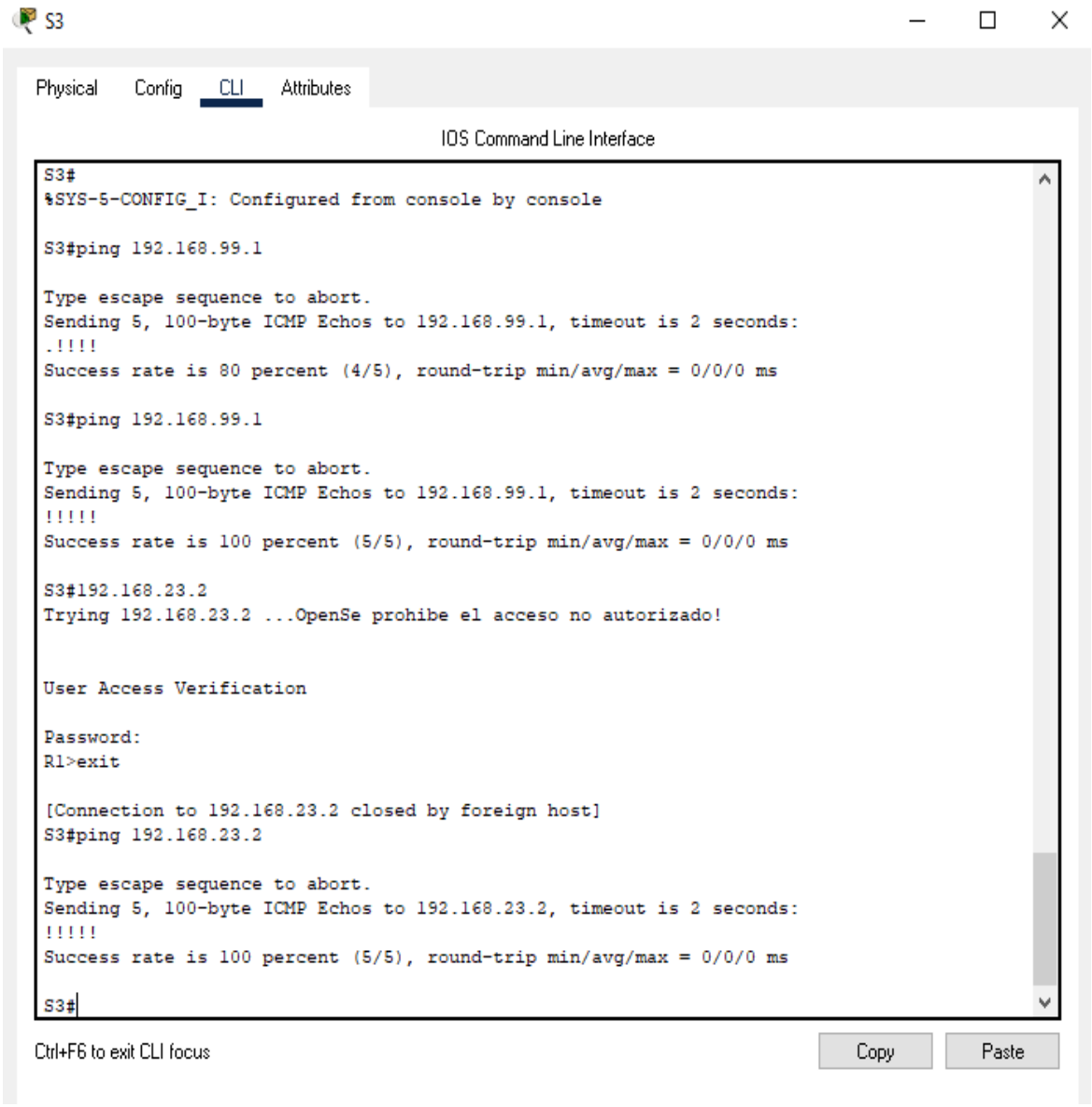


Figura 4. Ping de S1 a R1 con VLAN 99 y VLAN 21. Ingeniería de sistemas

PARTE 4: Configurar el protocolo de routing dinámico RIPv2

PASO 1: Configurar RIPv2 en el R1

Las tareas de configuración para R1 incluyen las siguientes:

Se configura el RIP version 2 en el router R1, donde se anunciarán las redes conectadas directamente las cuales son 172.16.1.0, 172.16.1.8, 192.168.21.0, 192.168.23.0, 192.168.99.0, después se establece todas las interfaces LAN como pasivas que son s0/0/0, g0/1 y por último se desactivan la sumarización automáticacon el código no auto-summary.

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	R1(config)#router rip R1(config-router)#version 2
Anunciar las redes conectadas directamente	R1(config-router)#network 172.16.1.0 R1(config-router)#network 172.16.1.8 R1(config-router)#network 192.168.21.0 R1(config-router)#network 192.168.23.0 R1(config-router)#network 192.168.99.0
Establecer todas las interfaces LAN como pasivas	R1(config-router)#passive-interface s0/0/0 R1(config-router)#passive-interface g0/1
Desactive la sumarización automática	R1(config-router)#no auto-summary

Tabla 3. Configuración RIPv2 *router 1*

PASO 2: Configurar RIPv2 en el R2

La configuración del R2 incluye las siguientes tareas:

Se configura el RIP version 2 en el router R2, donde se anunciarán las redes conectadas directamente las cuales son 10.10.10.0, 172.16.1.0, 172.16.2.0, después se establece la interface LAN loopback como pasiva y por último se desactivan la sumarización automáticacon el código no auto-summary.

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	R2(config)#router rip R2(config router)#version 2
Anunciar las redes conectadas directamente	R2(config-router)#network 10.10.10.0 R2(config-router)#network 172.16.1.0 R2(config-router)#network 172.16.2.0
Establecer la interfaz LAN (loopback) como pasiva	R2(config-router)#passive-interface loopback0
Desactive la sumarización automática.	R2(config-router)#no auto-summary

Tabla 12. Configuración RIPv2 *router 2*

PASO 3: Configurar RIPv3 en el R2

La configuración del R3 incluye las siguientes tareas:

Se configura el RIP version 2 en el router R3, donde se anunciarán las redes conectadas directamente las cuales son 172.16.2.0, 192.168.4.0, 192.168.5.0, 192.168.6.0, después se establecen las interfaces LAN loopback como pasiva y por último se desactivan la sumarización automáticacon el código no auto-summary.

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	R3(config)#router rip R3(config-router)#version 2
Anunciar redes IPv4 conectadas directamente	R3(config-router)#network 172.16.2.0 R3(config-router)#network 192.168.4.0 R3(config-router)#network 192.168.5.0 R3(config-router)#network 192.168.6.0
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	R3(config-router)#passive-interface loopback4 R3(config-router)#passive-interface loopback5 R3(config-router)#passive-interface loopback6
Desactive la sumarización automática.	R3(config-router)#no auto-summary

Tabla 13. Configuración RIPv2 *router 3*

PASO 4: Verificar la información de RIP

Verifique que RIP esté funcionando como se espera. Introduzca el comando de CLI adecuado para obtener la siguiente información

Pregunta	Respuesta
¿Con qué comando se muestran la ID del proceso RIP, la ID del router, las redes de routing y las interfaces pasivas configuradas en un router?	R1#show ip protocols
¿Qué comando muestra solo las rutas RIP?	R1#debug ip rip
¿Qué comando muestra la sección de RIP de la configuración en ejecución?	R1#show ip route

Tabla 14. Configuración RIP router 1

R1 SHOW IP PROTOCOLS

Se presenta la configuración de RIP en el router R1 para mostrar el protocolo de información de enrutamiento como el vector de distancia, por medio de la configuración show IP protocolos para que los muestre. En la figura se muestra el encaminamiento de las interfaces en su versión 2 y sus direcciones.

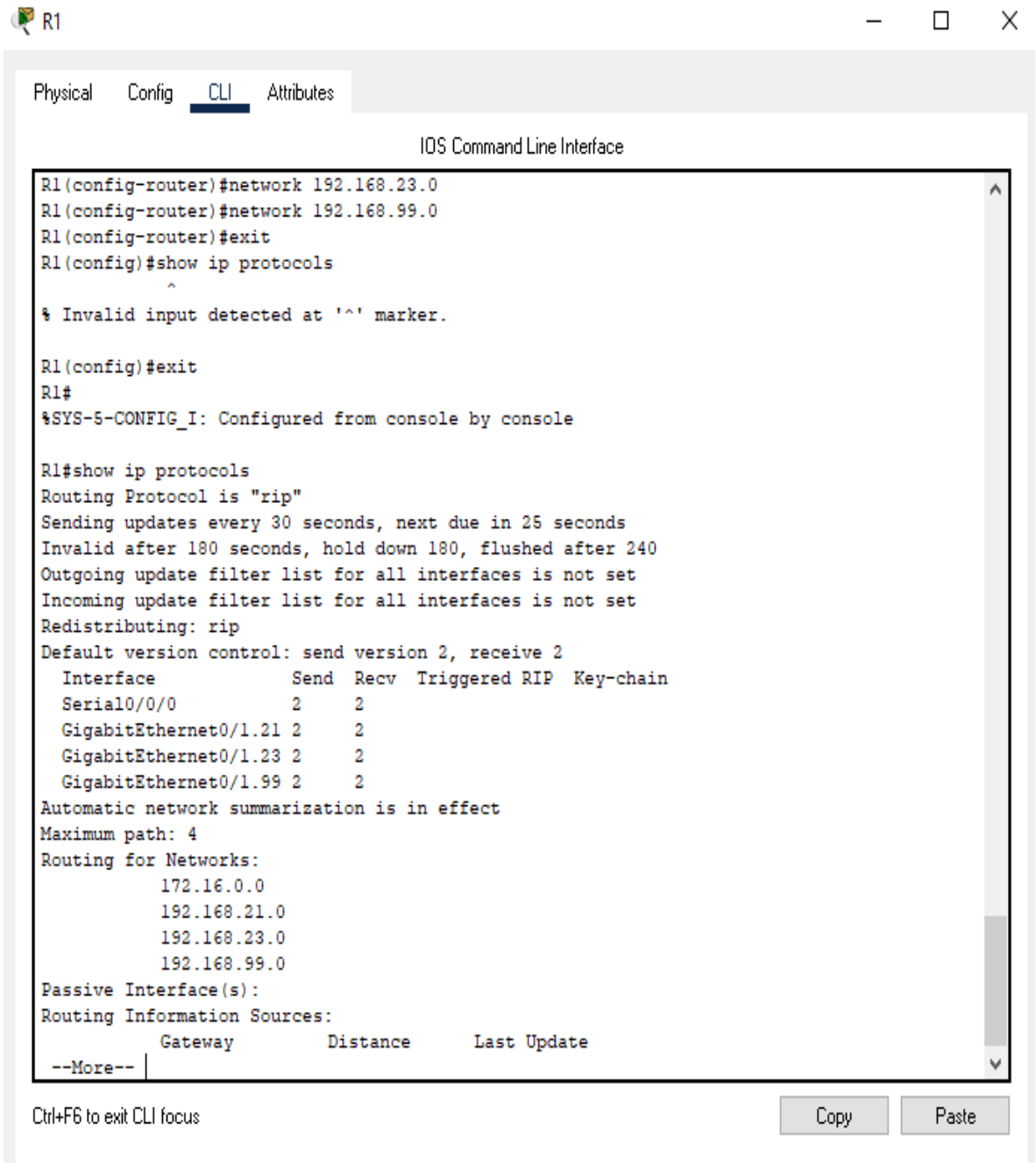


Figura 5. Show Ip protocos en R1. Ingeniería de sistemas

R1 DEBUG IP RIP

Se presenta la configuración el debug de IP RIP en el router R1 para mostrar las rutas RIP, por medio de la configuración debug IP RIP. En la figura se muestra las diferentes direcciones en los Gateways e interfaces.

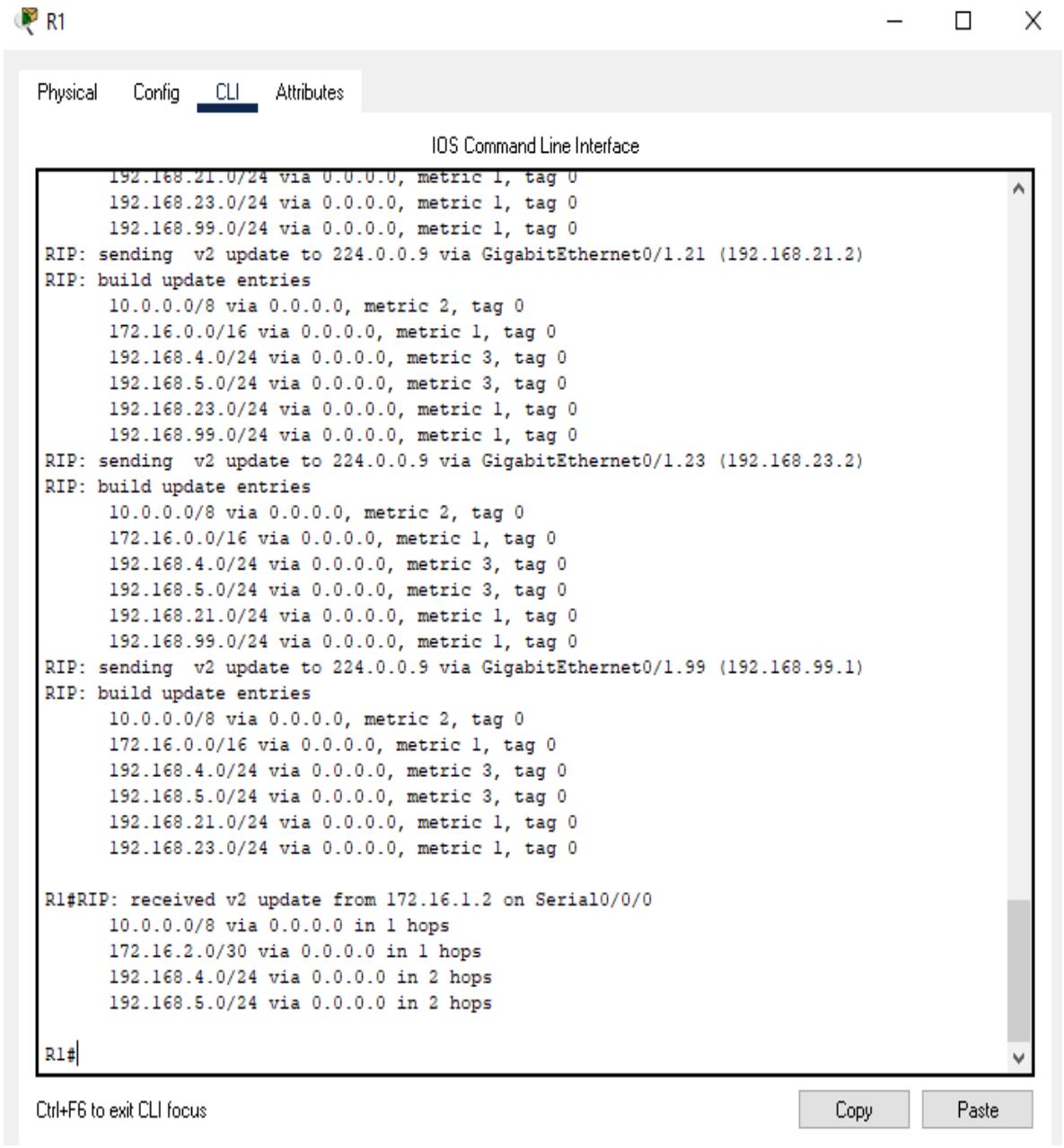


Figura 6. Debug Ip RIP en R1. Ingeniería de sistemas

R1 SHOW IP ROUTE

Se presenta la configuración el Ip route en el router R1 para mostrar la sección de RIP de la configuración en ejecución, por medio de la configuración show IP route. En la figura se verificar la información de enrutamiento que se utiliza para definir el reenvío de tráfico.

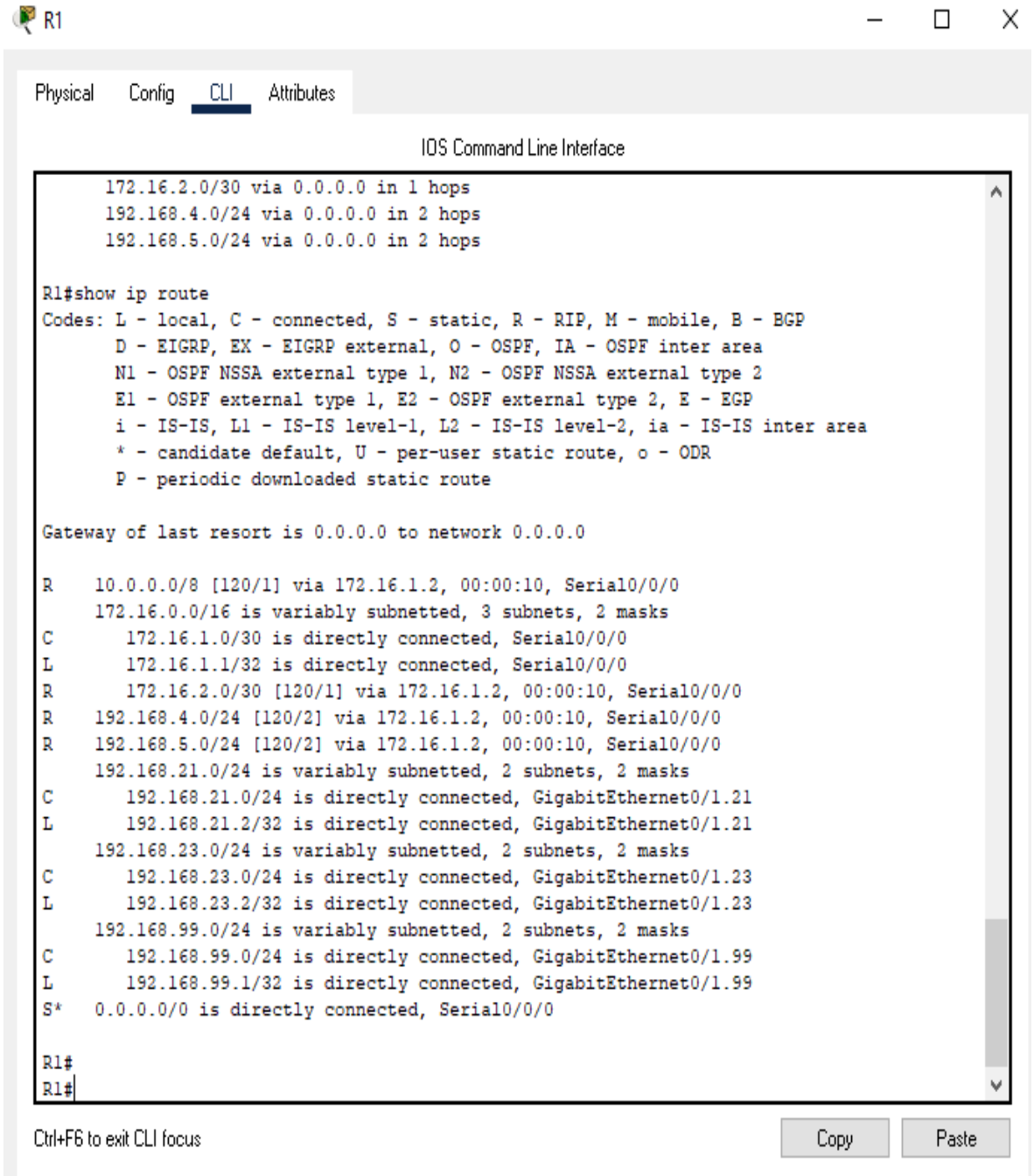


Figura 7. Debug Ip RIP en R1. Ingeniería de sistemas

PARTE 5: Implementar DHCP y NAT para IPv4

PASO 1: Configurar el R1 como servidor de DHCP para las VLAN 21 y 23

Las tareas de configuración para R1 incluyen las siguientes:

La próxima configuración se hace en el router R1 como servidor de DHCP para las VLAN 21 y 23 donde se reservan las primeras 20 direcciones IP en la VLAN 21 y se configuran como estáticas, también se hace lo mismo con la VLAN 23 y estas son las direcciones respectivamente 192.168.21.1 192.168.21.20, 192.168.23.1 192.168.23.20. También se crea un pool de DHCP para la VLAN 21 y 23 donde se da el nombre de los cargos de contador e ingeniero, también se configura un servidor DNS que en este caso es 10.10.10.10 y un nombre de dominio que es ccna-sa.com y por último se establece un gateway determinado que es 192.168.23.1.

Elemento o tarea de configuración	**Especificación**
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.20
Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas	R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.20
Crear un pool de DHCP para la VLAN 21.	R1(config)#ip dhcp pool ACCT R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#domain-name ccna-sa.com R1(dhcp-config)#default-router 192.168.21.1 R1(dhcp-config)#network 192.168.21.0 255.255.255.0
Crear un pool de DHCP para la VLAN 23	R1(config)#ip dhcp pool ENGNR R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#domain-name ccna-sa.com R1(dhcp-config)#default-router 192.168.23.1 R1(dhcp-config)#network 192.168.23.0 255.255.255.0

Tabla 15. Configuración DHCP y NAT *router 1*

PASO 2: Configurar la NAT estática y dinámica en el R2

La configuración del R2 incluye las siguientes tareas:

Se va a configurar la NAT estética y dinámica para el router R2 donde se comienza con una base de datos local y una cuenta de usuario en este caso el usuario es

Webuser y la contraseña cisco 12345 y el nivel de privilegio 15, después se habilita el servidor HTTP y se configura el servidor HTTP para utilizar la base de datos local para la autenticación por medio del código http autenticación local, después se crea una NAT estadística del servidor web por medio de la dirección global interna que es 209.165.200.229. Después se asignan las interfaz internas y externas para la NAT estática que es 10.10.10.10 209.165.200.229 y la interfaz externa g0/0 y interna g0/0. También se configurar la NAT dinámica dentro de una ACL privada que son 192.168.21.0 0.0.0.255, 192.168.23.0 0.0.0.255, 192.168.4.1 0.0.0.255, 192.168.5.1 0.0.0.255, 192.168.6.1 0.0.0.255. Por último, se define el pool de direcciones IP publicas 209.165.200.225 209.165.200.228 netmask 255.255.255.248 y se define la traducción de NAT dinámica nat inside source list 1 pool INTERNET.

Elemento o tarea de configuración	Especificación
Crear una base de datos local con una cuenta de usuario	R2(config)#user webuser privilege 15 secret cisco12345
Habilitar el servicio del servidor HTTP	R2(config)#ip http server
Configurar el servidor HTTP para utilizar la base de datos local para la autenticaci	R2(config)#ip http authentication loca
Crear una NAT estática al servidor web.	R2(config)#ip nat inside source static 10.10.10.10 209.165.200.229 R2(config)#interface g0/0 R2(config-if)#ip nat outside R2(config-if)#interface g0/0 R2(config-if)#ip nat inside
Asignar la interfaz interna y externa para la NAT estática	R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.4.1 0.0.0.255 R2(config)#access-list 1 permit 192.168.5.1 0.0.0.255 R2(config)#access-list 1 permit 192.168.6.1 0.0.0.255 int f0/1
Configurar la NAT dinámica dentro de una ACL privada	R2(config)#ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask 255.255.255.248 R2(config)#ip nat inside source list 1 pool INTERNET
Defina el pool de direcciones IP públicas utilizables.	El conjunto de direcciones incluye: 209.165.200.225-209.165.200.228
Definir la traducción de NAT dinámica	Ip nat inside source list 1 pool INTER

Tabla 16. Configuración NAT estática y dinámica *router 2*

PASO 3: Verificar el protocolo DHCP y la NAT estática

Utilice las siguientes tareas para verificar que las configuraciones de DHCP y NAT estática funcionen de forma correcta. Quizá sea necesario deshabilitar el firewall de las computadoras para que los pings se realicen correctamente.

Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	Sucessfull
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	Sucessfull
Verificar que la PC-A pueda hacer ping a la PC-C **Nota:** Quizá sea necesario deshabilitar el firewall de la PC.	Sucessfull
Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.237) Iniciar sesión con el nombre de usuario **webuser** y la contraseña **cisco12345**	Packer tracer no soporta la configuración de http server

Tabla 17. Verificación de DHCP y la NAT estática

PC-A

En la figura se demuestra la verificación que la PC-A haya adquirido información de IP del servidor de DHCP con la dirección IPV4.

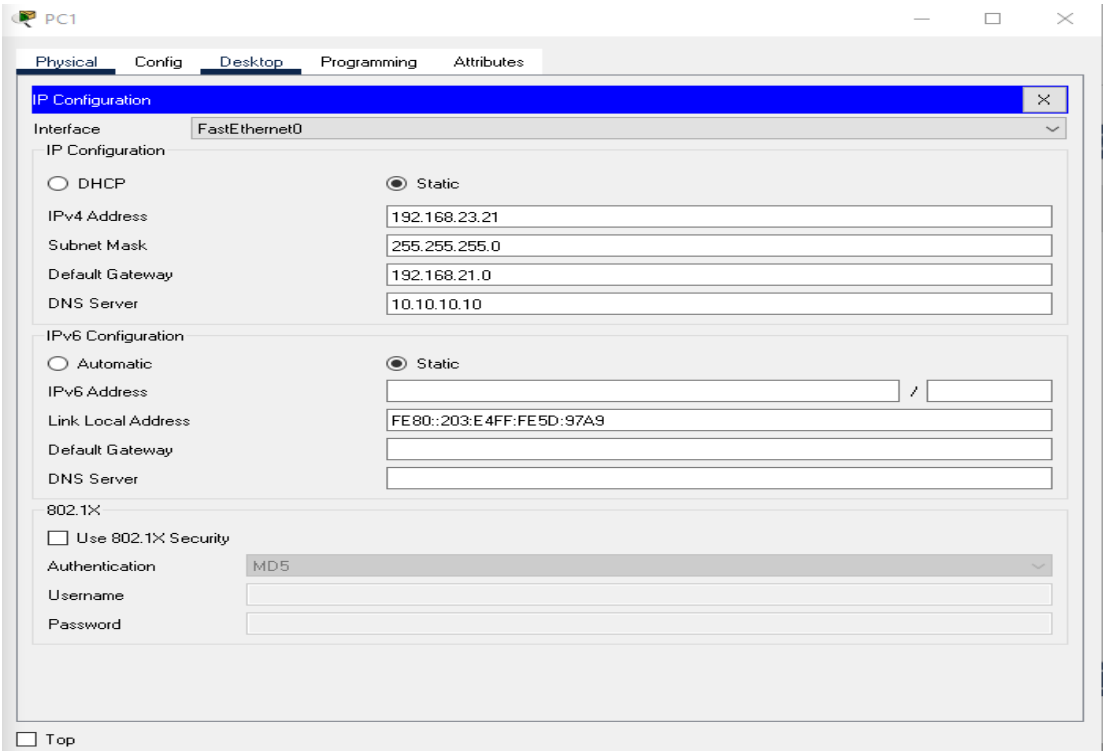


Figura 8. Configuración DHCP para la PC-A. Ingeniería de sistemas

PC-B

En la figura se demuestra la verificación que la PC-B haya adquirido información de IP del servidor de DHCP con la dirección IPV4,

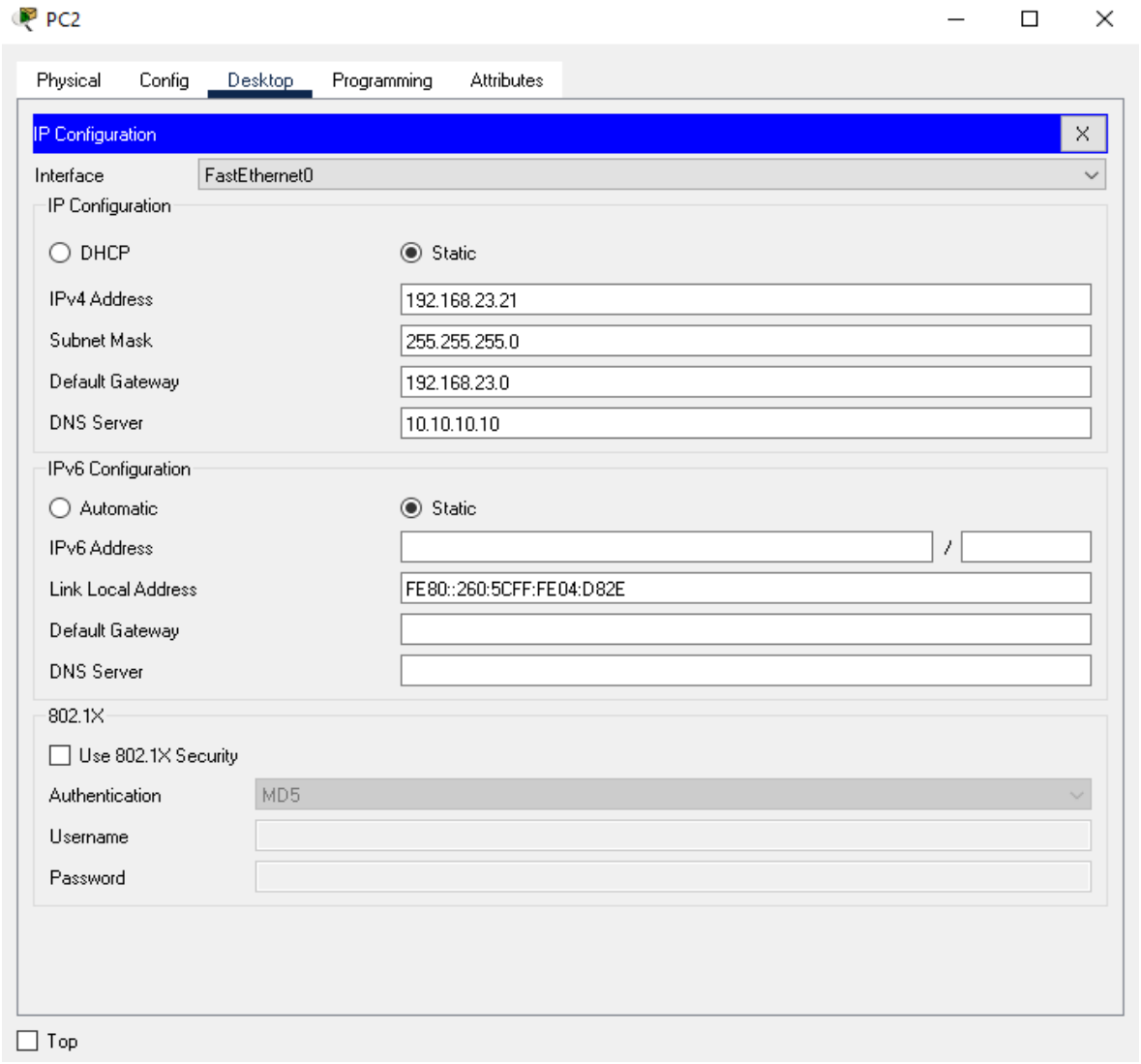


Figura 9. Configuración DHCP para la PC-B. Ingeniería de sistemas

PARTE 6: Configurar NTP

Para la siguiente parte se busca configurar la NTP para el router R2 donde se ajusta la fecha y la hora en R2 a 9:00:00 am 5 marzo 2016, también se configura R2 como un maestro NTP con el código ntp master Stratum 5 y se configura la R1 como cliente NTP 172.16.1.2, después se configura R1 para actualizaciones de calendario periódico con hora NTP con el código ntp update-calendar y por último se configura la NTP en R1 con el código do show ntp status.

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2.	Clock set 9:00:00 am 5 marzo 2016
Configure R2 como un maestro NTP.	R2(config)#ntp master Stratum 5
Configurar R1 como un cliente NTP.	R1(config)#ntp server 172.16.1.2
Configure R1 para actualizaciones de calendario periódicas con hora NTP.	R1(config)#ntp update-calendar
Verifique la configuración de NTP en R1.	R1(config)#do show ntp status

Tabla 18. Configuración de NTP

PARTE 7: Configurar y verificar las listas de control de acceso (ACL**)**

PASO 1: Restringir el acceso a las líneas VTY en el R2

Para el siguiente paso se restringe el acceso a las líneas VTY en el router R2, primero se configura una lista de acceso con nombre para permitir que solo R1 esablezca una conecxion Telnet con el router R2 el nombre es ADMIN-MGT, depsues se aplica la ACL con nombre a las líneas de VTY **(**line vty 0 4) y se permite acceso por Telnet a las líneas de

Elemento o tarea de configuración	Especificación
Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2	R2(config)#ip access-list standard ADMIN-MGT R2(config-std-nacl)#permit host 172.16.1.1
Aplicar la ACL con nombre a las líneas VTY	R2(config)#line vty 0 4
Permitir acceso por Telnet a las líneas de VTY	R2(config-line)#access-class ADMIN-MGT in
Verificar que la ACL funcione como se espera	Sucessfull

Tabla 19. Restringir el acceso a las líneas VTY en el R2

PASO 2: Introducir el comando de CLI adecuado que se necesita para mostrar lo siguiente.

Descripción del comando	Entrada del estudiante (comando)
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	Router(config)#show access-list
Restablecer los contadores de una lista de acceso	Router(config)#clear access-list counters
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	Router(config)#interface Fa0/1 Router(config-if)#ip access-group 1 out
¿Con qué comando se muestran las traducciones NAT?	Router(config)#show ip nat translations **Nota:** Las traducciones para la PC-A y la PC-C se agregaron a la tabla cuando la computadora de Internet intentó hacer ping a esos equipos en el paso 2. Si hace ping a la computadora de Internet desde la PC-A o la PC- C, no se agregarán las traducciones a la tabla debido al modo de simulación de Internet en la red.
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	Router(config)#clear ip nat translation

Tabla 19. Comando de CLI

CONCLUSIONES

Por medio de las redes creadas se entendió como se puede conectar una empresa, se aprendió a programar claves y asegurar las redes para empezar, pero después se en rutaron se conectaron y por medio de direcciones ip y todo se puedo comprobar por medio de pings que generan una red funcionaria. También se realiza un numero amplio de tareas importantes para el desarrollo de los ejercicios presentados, donde se ejecutaron funciones como la de verificar conexiones entre dispositivos. También se logró conocer que con los ACLs de IPv6.

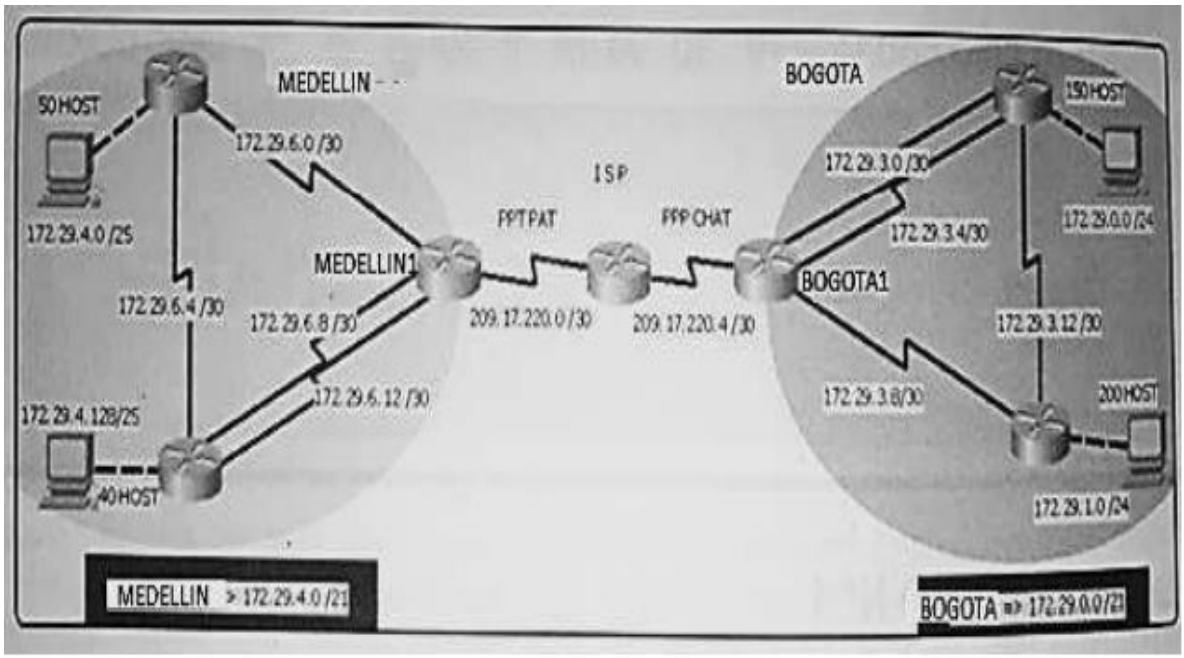
Es interesante la configuración del NAT ya que programa el tiempo de las ejecuciones. Se logra aprender y permitir el direccionamiento mediante interfaces específicas en el router que estemos trabajando, y como evidenciamos en la práctica podremos evitar fallas generadas por presencia de bucles en los hosts. La configuración NAT dinámica que se implementó funcionan muy bien en la configuración de redes en empresas ya que sirve para conectar varias redes internas a Internet mediante varias direcciones IP públicas. Se aprendió a configurar los direccionamientos de IPV6 en host y la configuración de protocolos DHCPv6 que establece automáticamente los direccionamientos a los hosts

Esta actividad fue basada para entender los funcionamientos de redes en las empresas desde un mismo punto o diferentes puntos y es complejo entender cómo funcionan estas redes, pero al comprender lo ya mencionado se puede comprender sus funciones.

ESCENARIO 2

Una empresa posee sucursales distribuidas en las ciudades de Bogotá y Medellín, en donde el estudiante será el administrador de la red, el cual deberá configurar e interconectar entre sí cada uno de los dispositivos que forman parte del escenario, acorde con los lineamientos establecidos para el direccionamiento IP, protocolos de enrutamiento y demás aspectos que forman parte de la topología de red.

TOPOLOGIA RED



Este escenario plantea el uso de OSPF como protocolo de enrutamiento, considerando que se tendrán rutas por defecto redistribuidas; asimismo, habilitar el encapsulamiento PPP y su autenticación.

Los routers Bogota2 y medellin2 proporcionan el servicio DHCP a su propia red LAN y a los routers 3 de cada ciudad.

Debe configurar PPP en los enlaces hacia el ISP, con autenticación. Debe habilitar NAT de sobrecarga en los routers Bogota1 y medellin1.

DESARROLLO

Como trabajo inicial se debe realizar lo siguiente.

- Realizar las rutinas de diagnóstico y dejar los equipos listos para su configuración (asignar nombres de equipos, asignar claves de seguridad, etc).

- Realizar la conexión física de los equipos con base en la topología de red.

CONFIGURACION ROUTER:

Se desactiva la búsqueda DNS con el comando no ip domain-lookup para que sea rápida y no sea insensible, se configura el router, después se crea una contraseña de acceso de exclusivo privilegiado llamada class y contraseña de acceso a la consola cual es cisco y la contraseña de Telner la cual es cisco también. Después se cifran las contraseñas de texto no cifrado por medio del código service password-encryption, y después se configura un mensaje de acceso no autorizado con un banner motd. Por ultimo, se crea el hostname ISP

Router(config)#no ip domain-lookup
Router(config)#service password-encryption
Router(config)#enable secret class
Router(config)#banner motd # Prohibido el acceso no autorizado!#
Router(config)#line console 0
Router(config-line)#password cisco
Router(config-line)#login
Router(config-line)#line vty 0 4
Router(config-line)#password cisco
Router(config-line)#login Router(config-line)#exit
Router(config)# Hostname ISP

Configurar la topología de red, de acuerdo con las siguientes especificaciones.

PARTE 1: Configuración del enrutamiento

a. Configurar el enrutamiento en la red usando el protocolo OSPF versión 2, declare la red principal, desactive la sumarización automática.

Se configuran los routers Bogota1, Bogota2, Bogota3 y Medellin1, Medellin2, Medillin3 con sus direcciones de enrutamiento de la red, usnados los protocolos OSPF versión 2 y se declaran las redes principales, por último se desactivan la sumarizacion automática para cada router

BOGOTA1(config)#router ospf 1
BOGOTA1(config-router)#router-id 1.1.1.1

```
BOGOTA1(config-router)#network 172.29.3.0 0.0.0.3 area 0
BOGOTA1(config-router)#network 172.29.3.4 0.0.0.3 area 0
BOGOTA1(config-router)#network 172.29.3.8 0.0.0.3 area 0
BOGOTA1(config-router)#network 209.17.220.4 0.0.0.3 area 0
BOGOTA1(config-router)#no auto-summary

BOGOTA2(config)#router ospf 1
BOGOTA2(config-router)#router-id 3.3.3.3
BOGOTA2(config-router)#network 172.29.1.0 0.0.0.255 area 0
BOGOTA2(config-router)#network 172.29.3.8 0.0.0.3 area 0
BOGOTA2(config-router)#network 172.29.3.8 0.0.0.3 area 0
BOGOTA2(config-router)#network 172.29.3.12 0.0.0.3 area 0
BOGOTA2(config-router)#no auto-summary
BOGOTA2(config-router)#passive-interface g0/0

BOGOTA3(config)#router ospf 1
BOGOTA3(config-router)#router-id 4.4.4.4
BOGOTA3(config-router)#network 172.29.0.0 0.0.0.255 area 0
BOGOTA3(config-router)#network 172.29.3.0 0.0.0.3 area 0
BOGOTA3(config-router)#network 172.29.3.4 0.0.0.3 area 0
BOGOTA3(config-router)#network 172.29.3.12 0.0.0.3 area 0
BOGOTA3(config-router)#no auto-summary
BOGOTA3(config-router)#passive-interface g0/0

MEDELLIN1(config)#router ospf 1
MEDELLIN1(config-router)#router-id 2.2.2.2
MEDELLIN1(config-router)#network 172.29.6.0 0.0.0.3 area 0
MEDELLIN1(config-router)#network 172.29.6.4 0.0.0.3 area 0
MEDELLIN1(config-router)#network 172.29.6.8 0.0.0.3 area 0
MEDELLIN1(config-router)#network 209.17.220.0 0.0.0.3 area 0
MEDELLIN1(config-router)#no auto-summary

MEDELLIN2(config)#router ospf 1
MEDELLIN2(config-router)#router-id 5.5.5.5
MEDELLIN2(config-router)#network 172.29.4.0 0.0.0.255 area 0
MEDELLIN2(config-router)#network 172.29.6.0 0.0.0.3 area 0
MEDELLIN2(config-router)#network 172.29.6.12 0.0.0.3 area 0
MEDELLIN2(config-router)#no auto-summary
MEDELLIN2(config-router)#passive-interface g0/0 46

MEDELLIN3(config)#router ospf 1
MEDELLIN3(config-router)#router-id 6.6.6.6
MEDELLIN3(config-router)#network 172.29.4.0 0.0.0.255 area 0
MEDELLIN3(config-router)#network 172.29.6.4 0.0.0.3 area 0
MEDELLIN3(config-router)#network 172.29.6.8 0.0.0.3 area 0
```

```
MEDELLIN3(config-router)#network 172.29.6.12 0.0.0.3 area 0
MEDELLIN3(config-router)#passive-interface g0/0
MEDELLIN3(config-router)#no auto-summary
```

b. Los routers Bogota1 y Medellín deberán añadir a su configuración de enrutamiento una ruta por defecto hacia el ISP y, a su vez, redistribuirla dentro de las publicaciones de OSPF.

Se configuran los routers Bogota1 y Medellin1 con su enrutamiento ip route 0.0.0.0 0.0.0.0 serial0/0/0 y ip route 0.0.0.0 0.0.0.0 serial0/0/1 respectivamente. Se traza una ruta por defecto hacia el router ISP donde se redistribuirá dentro de publicaciones de OSPF.

```
BOGOTA1(config)#ip route 0.0.0.0 0.0.0.0 serial0/0/0
BOGOTA1(config)#router ospf 1
BOGOTA1(config-router)#default-information originate
```

```
MEDELLIN1(config)#ip route 0.0.0.0 0.0.0.0 serial0/0/1
MEDELLIN1(config)#router ospf 1
MEDELLIN1(config-router)#default-information originate
```

c. El router ISP deberá tener una ruta estática dirigida hacia cada red interna de Bogotá y Medellín para el caso se sumarizan las subredes de cada uno a /22.

Se configura el router ISP con una ruta estática ip route 172.29.4.0 255.255.252.0 serial0/0/1 a Bogotá y ip route 172.29.0.0 255.255.252.0 serial0/0/0 a Medellín

```
ISP(config)#ip route 172.29.4.0 255.255.252.0 serial0/0/1
ISP(config)#ip route 172.29.0.0 255.255.252.0 serial0/0/0
```

PARTE 2: Tabla de Enrutamiento.

a. Verificar el balanceo de carga que presentan los routers.

b. Verificar la tabla de enrutamiento en cada uno de los routers para comprobar las redes y sus rutas.
c. Obsérvese en los routers Bogotá1 y Medellín1 cierta similitud por su ubicación, por tener dos enlaces de conexión hacia otro router y por la ruta.

d. Los routers Medellín2 y Bogotá2 también presentan redes conectadas directamente y recibidas mediante OSPF.

e. Las tablas de los routers restantes deben permitir visualizar rutas redundantes para el caso de la ruta por defecto.

f. El router ISP solo debe indicar sus rutas estáticas adicionales a las directamente conectadas.

ISP

Se presenta la configuración el Ip route en el router ISP para mostrar la sección de RIP de la configuración en ejecución, por medio de la configuración show IP route. En la figura se verificar la información de enrutamiento que se utiliza para definir el reenvío de tráfico.

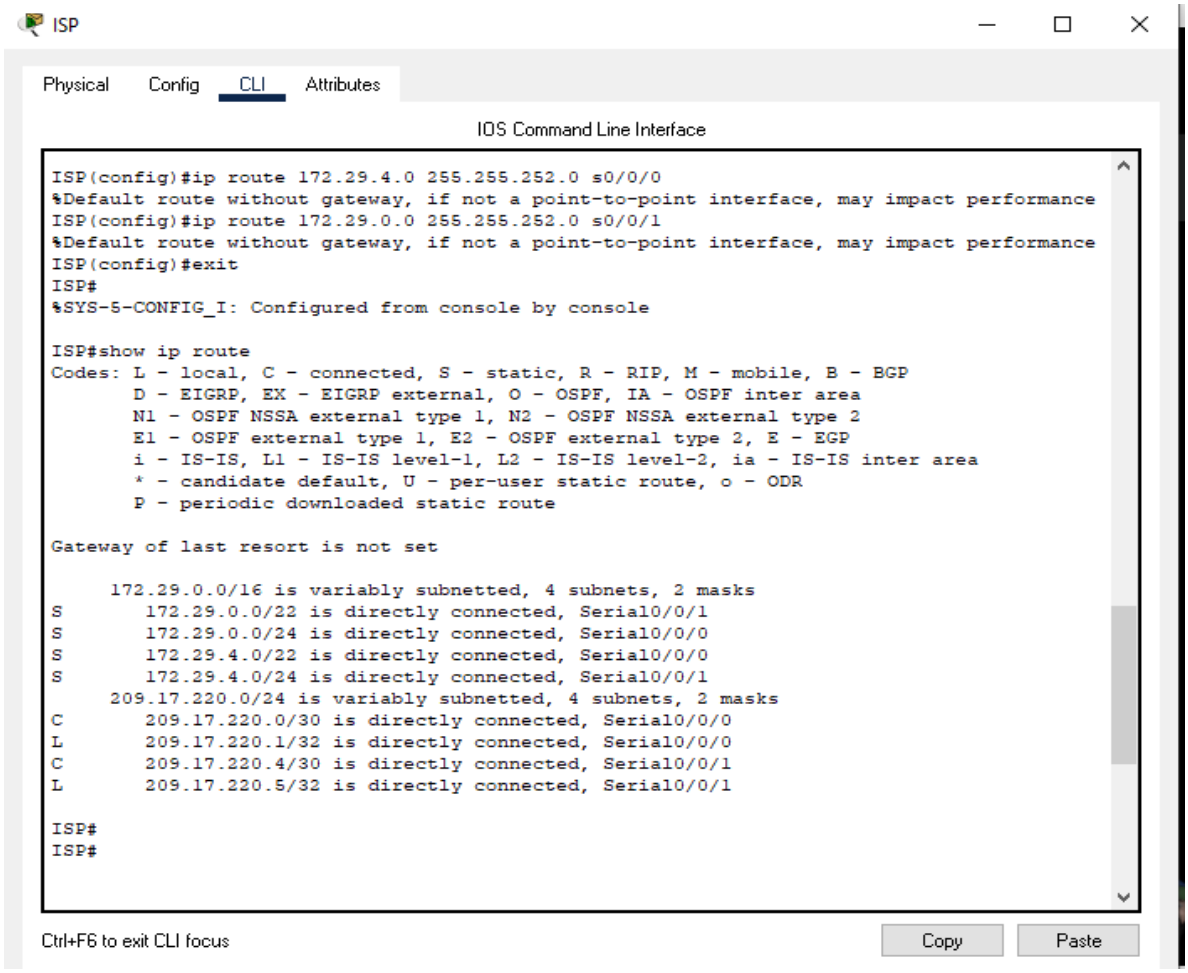


Figura 10. Show IP route del router ISP. Ingeniería de sistemas

MEDELLIN1

Se presenta la configuración el Ip route en el router MEDELLIN1 para mostrar la sección de RIP de la configuración en ejecución, por medio de la configuración show IP route. En la figura se verificar la información de enrutamiento que se utiliza para definir el reenvío de tráfico.

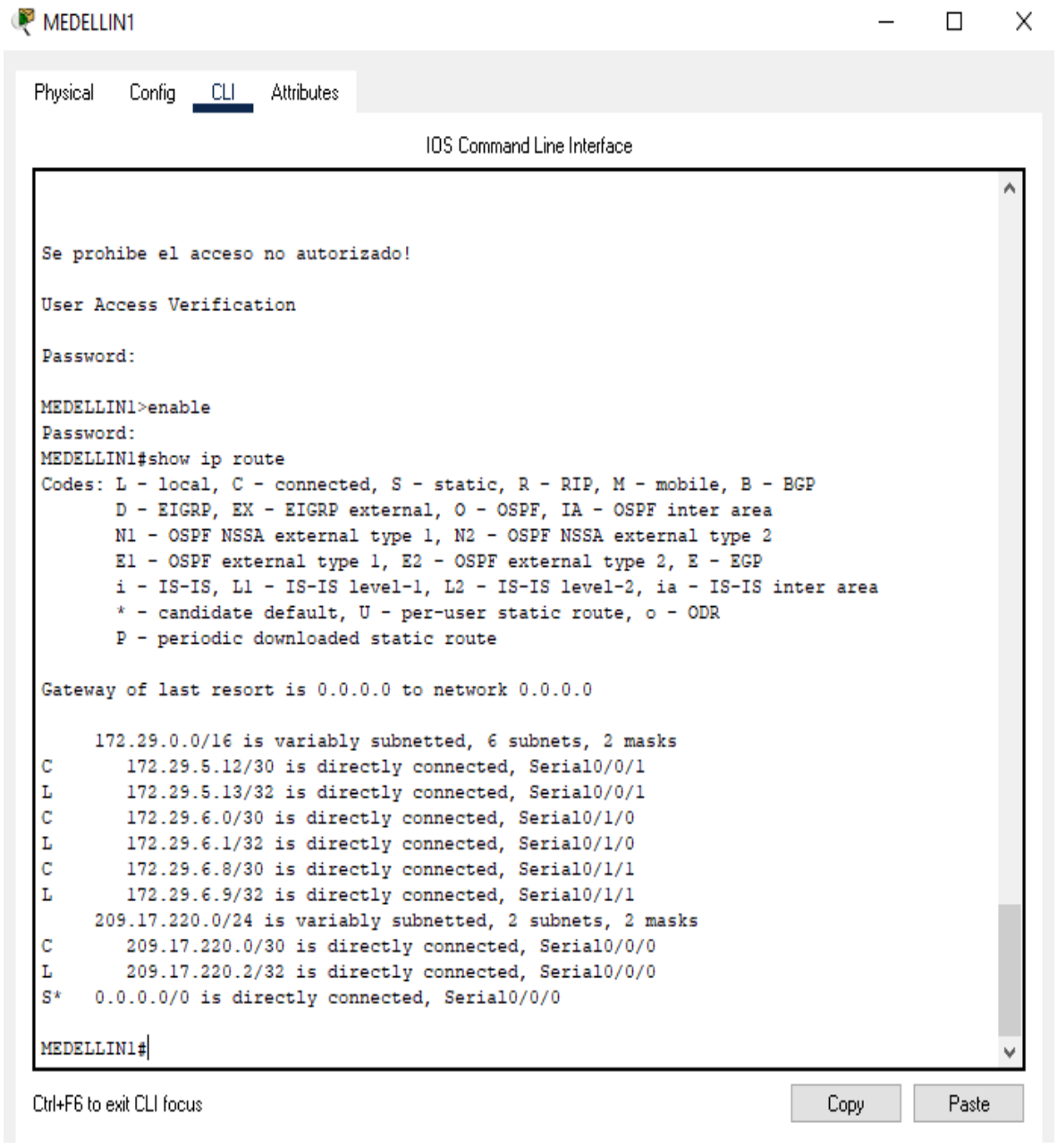


Figura 10. Show IP route del router MEDELLIN1. Ingeniería de sistemas

MEDELLIN2

Se presenta la configuración el Ip route en el router MEDELLIN2 para mostrar la sección de RIP de la configuración en ejecución, por medio de la configuración show IP route. En la figura se verificar la información de enrutamiento que se utiliza para definir el reenvío de tráfico.

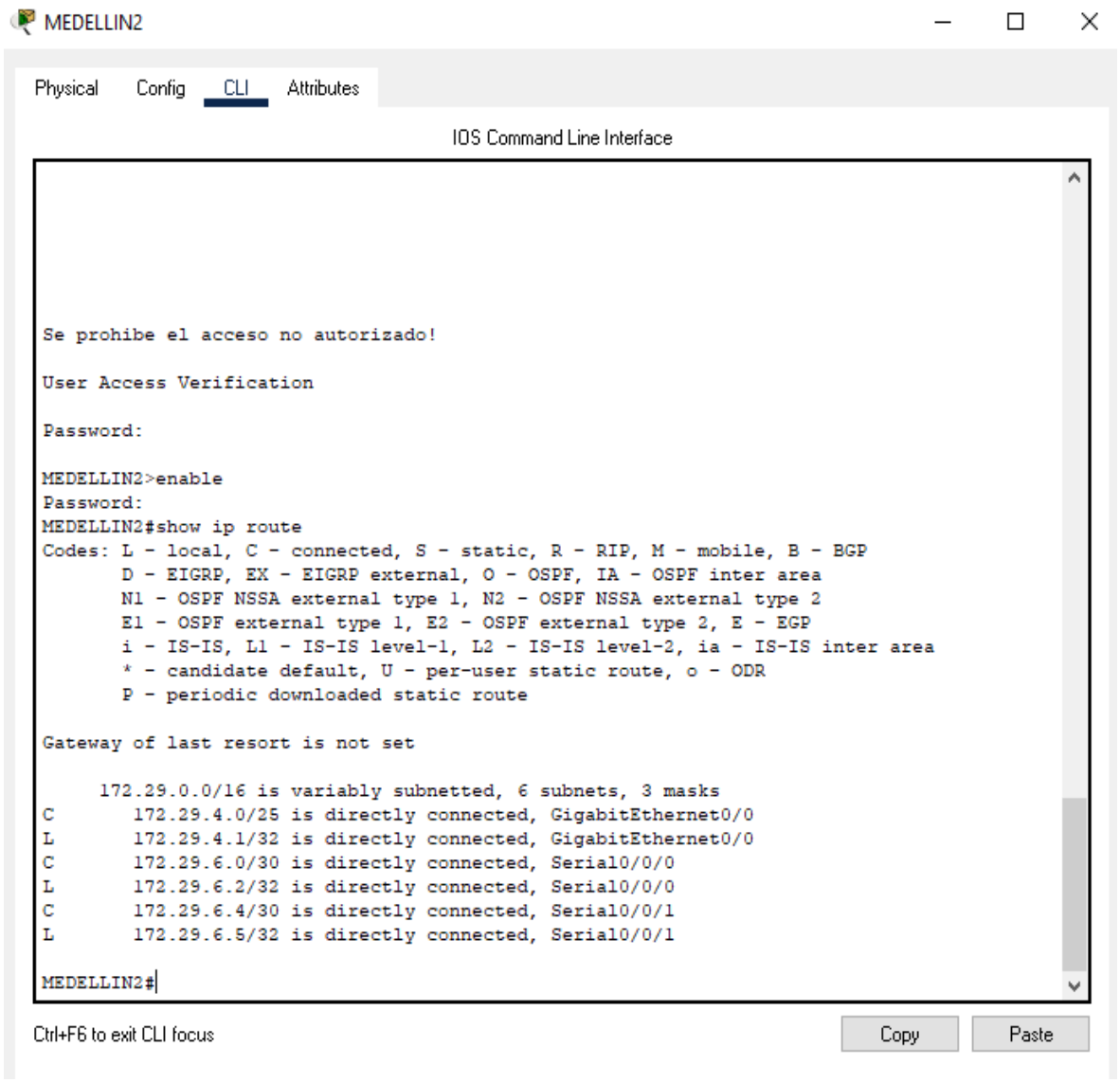


Figura 11. Show IP route del router MEDELLIN2. Ingeniería de sistemas

MEDELLIN3

Se presenta la configuración el Ip route en el router MEDELLIN3 para mostrar la sección de RIP de la configuración en ejecución, por medio de la configuración show IP route. En la figura se verificar la información de enrutamiento que se utiliza para definir el reenvío de tráfico.

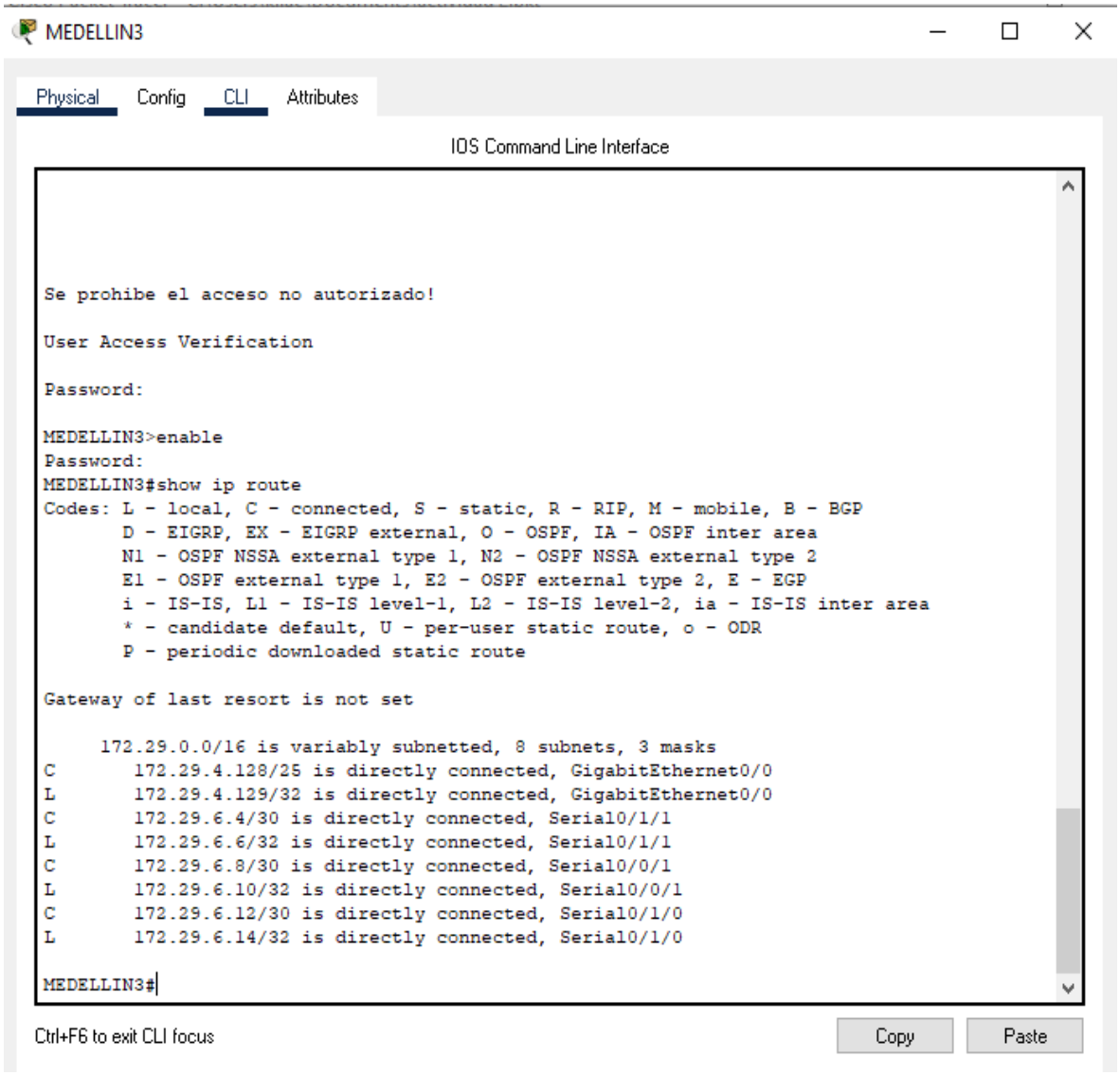


Figura 12. Show IP route del router MEDELLIN3. Ingeniería de sistemas

BOGOTA1

Se presenta la configuración el Ip route en el router BOGOTA1 para mostrar la sección de RIP de la configuración en ejecución, por medio de la configuración show IP route. En la figura se verificar la información de enrutamiento que se utiliza para definir el reenvío de tráfico.

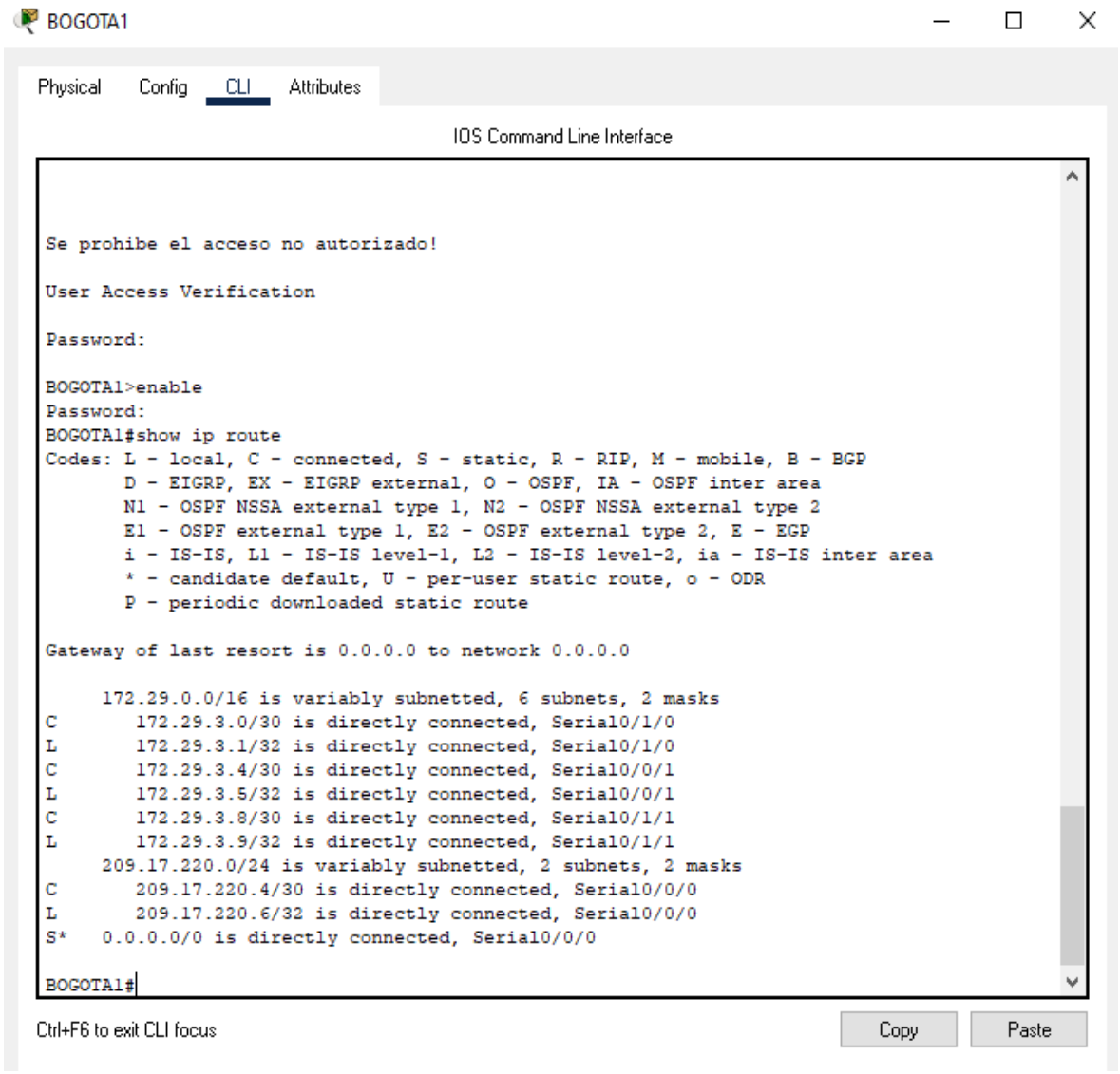


Figura 13. Show IP route del router BOGOTA1. Ingeniería de sistemas

BOGOTA2

Se presenta la configuración el Ip route en el router BOGOTA2 para mostrar la sección de RIP de la configuración en ejecución, por medio de la configuración show IP route. En la figura se verificar la información de enrutamiento que se utiliza para definir el reenvío de tráfico.

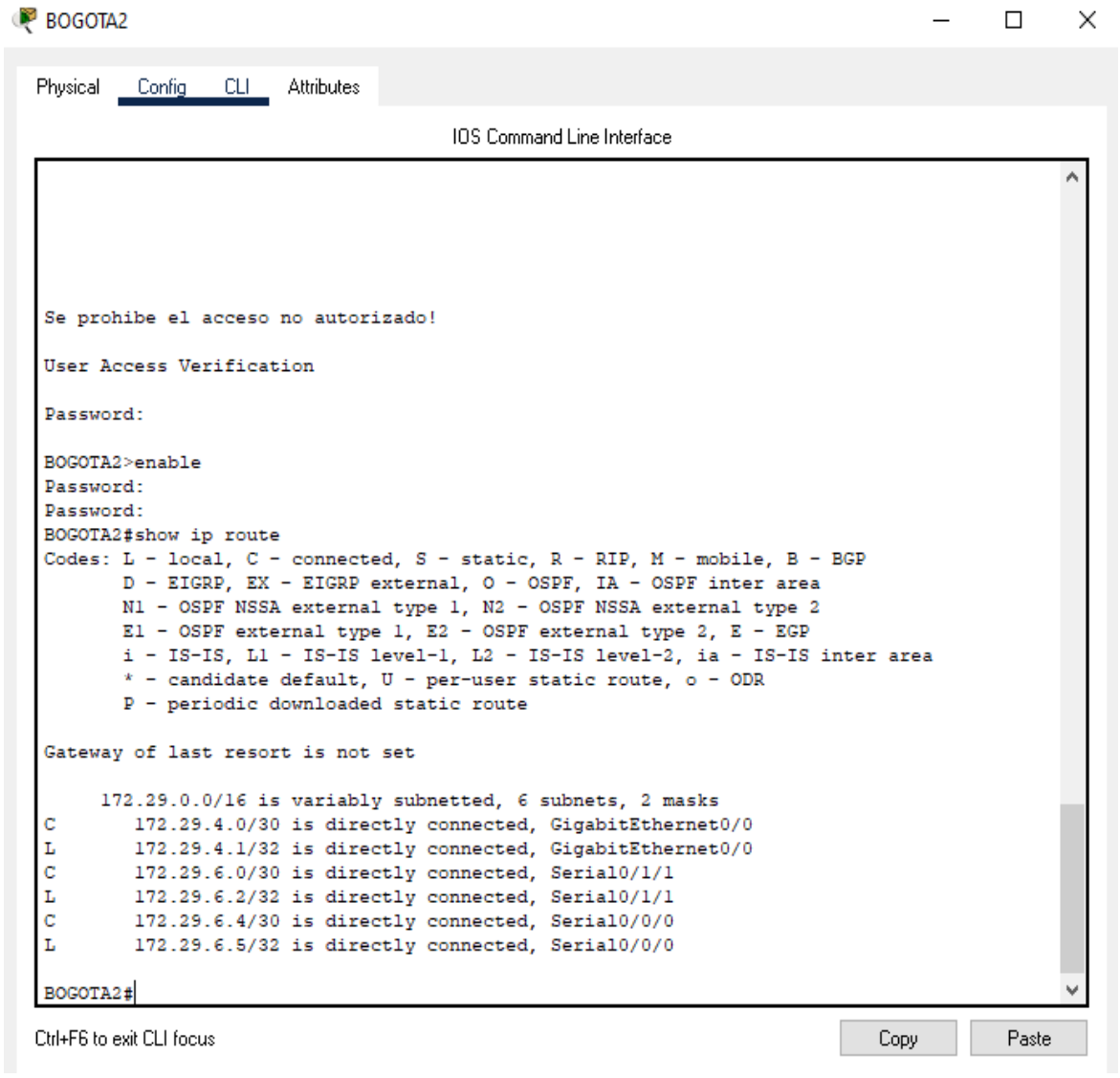


Figura 14. Show IP route del router BOGOTA2. Ingeniería de sistemas

BOGOTA3

Se presenta la configuración el Ip route en el router BOGOTA3 para mostrar la sección de RIP de la configuración en ejecución, por medio de la configuración show IP route. En la figura se verificar la información de enrutamiento que se utiliza para definir el reenvío de tráfico.

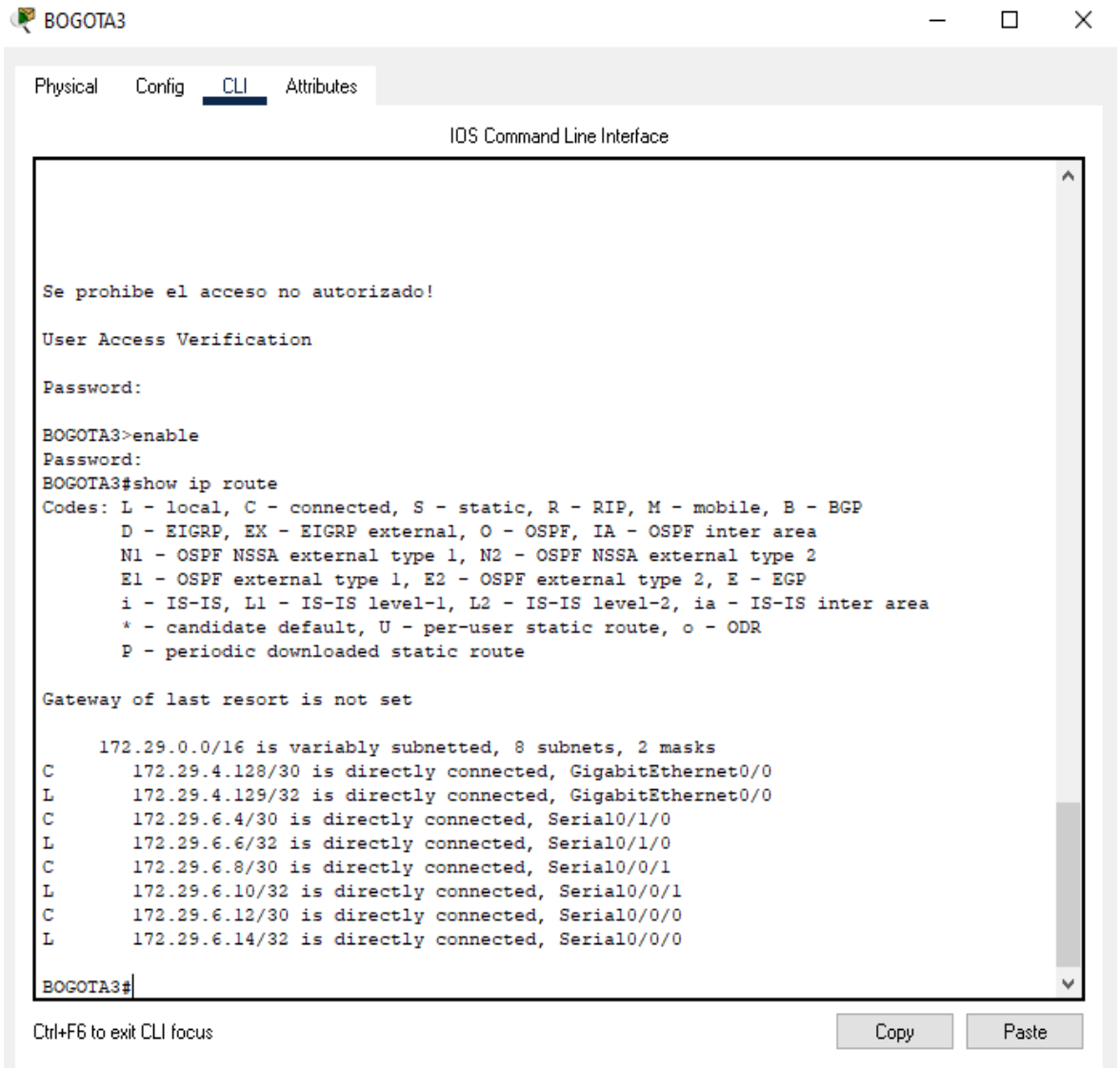


Figura 15. Show IP route del router BOGOTA3. Ingeniería de sistemas

PARTE 3: Deshabilitar la propagación del protocolo OSPF.

a. Para no propagar las publicaciones por interfaces que no lo requieran se debe deshabilitar la propagación del protocolo OSPF, en la siguiente tabla se indican las interfaces de cada router que no necesitan desactivación.

ROUTER	INTERFAZ
Bogota1	SERIAL0/0/1; SERIAL0/1/0; SERIAL0/1/1
Bogota2	SERIAL0/0/0; SERIAL0/0/1
Bogota3	SERIAL0/0/0; SERIAL0/0/1; SERIAL0/1/0
Medellín1	SERIAL0/0/0; SERIAL0/0/1; SERIAL0/1/1
Medellín2	SERIAL0/0/0; SERIAL0/0/1
Medellín3	SERIAL0/0/0; SERIAL0/0/1; SERIAL0/1/0
ISP	No lo requiere

BOGOTA3
BOGOTA3(config)#route OSPF 1
BOGOTA3(config-router) #passive-interface s0/1/1

MEDELLIN3
MEDELLIN3(config)#route OSPF 1
MEDELLIN3(config-router) #passive-interface s0/1/1

PARTE 4: Verificación del protocolo OSPF.

a. Verificar y documentar las opciones de enrutamiento configuradas en los routers, como el passive interface para la conexión hacia el ISP, la versión de OSPF y las interfaces que participan de la publicación entre otros datos.

MEDELLIN1

Se presenta la configuración de protocolo OSPF en el router MEDELLIN1 para mostrar el protocolo de información de enrutamiento como el vector de distancia, por medio de la configuración show IP protocolos para que los muestre. En la figura se muestra el encaminamiento de las interfaces en su versión 2 y sus direcciones.

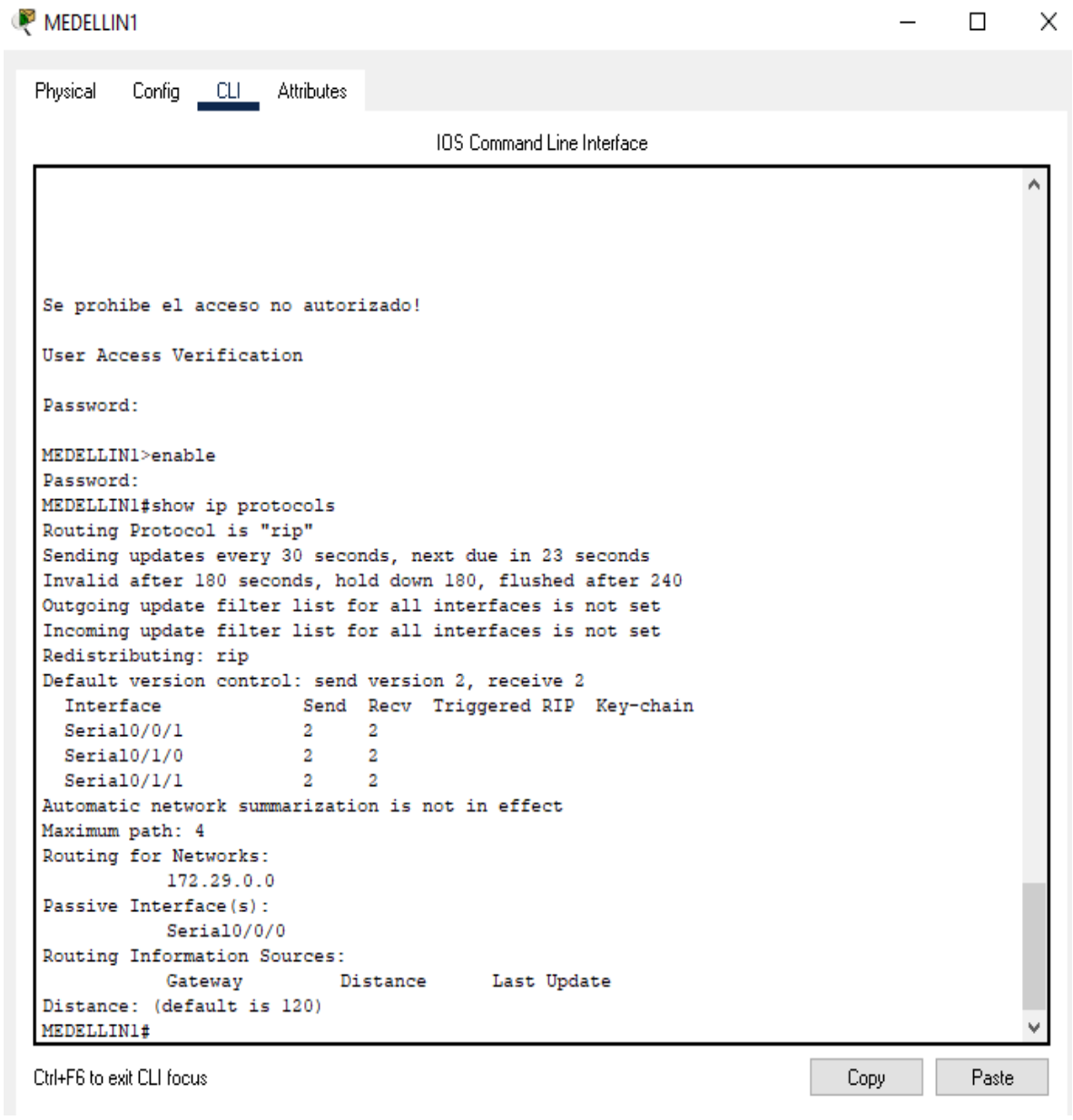


Figura 16. Show IP protocols on router MEDELLIN1. Ingeniería de sistemas

MEDELLIN2

Se presenta la configuración de protocolo OSPF en el router MEDELLIN2 para mostrar el protocolo de información de enrutamiento como el vector de distancia, por medio de la configuración show IP protocolos para que los muestre. En la figura se muestra el encaminamiento de las interfaces en su versión 2 y sus direcciones.

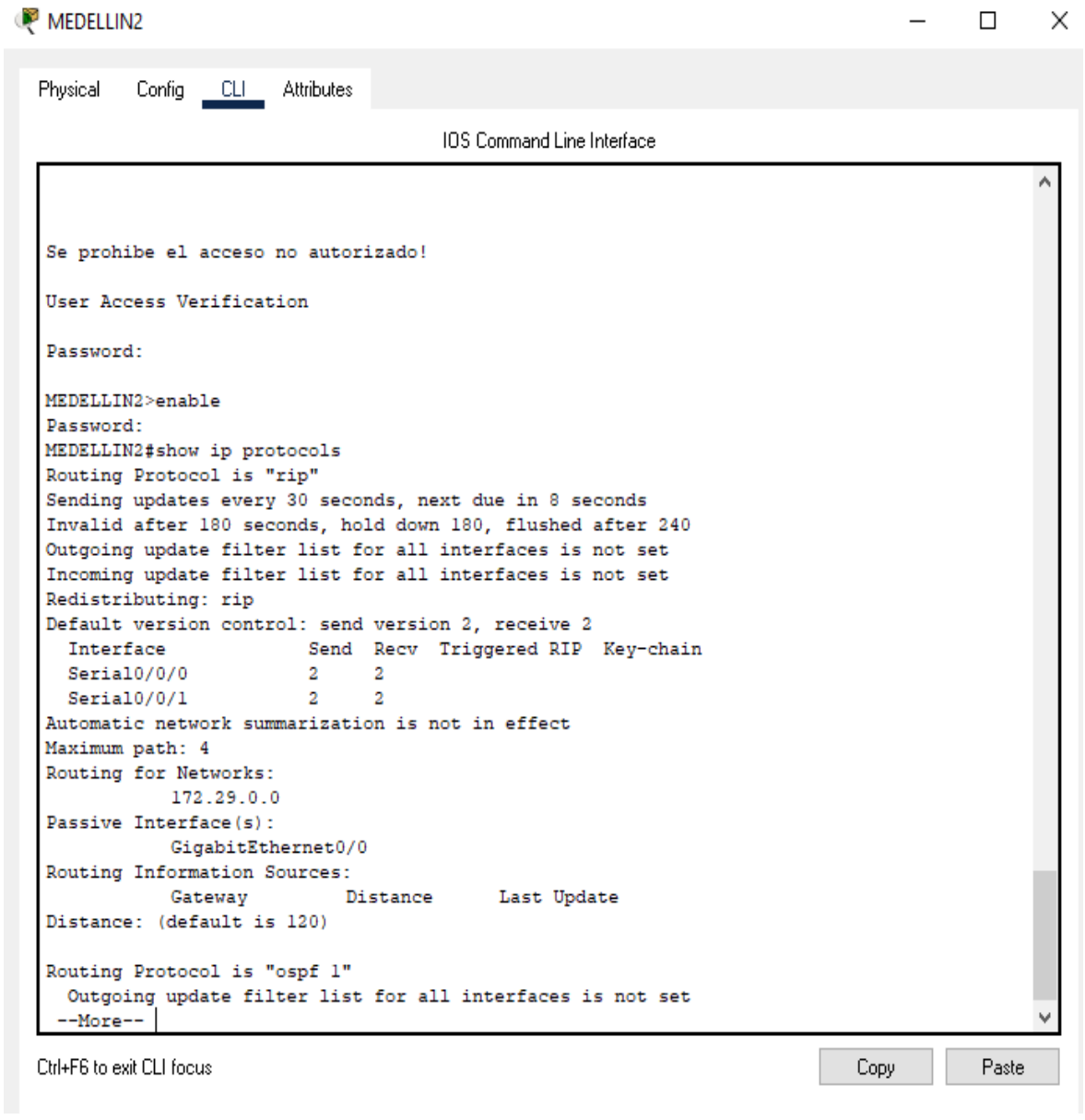


Figura 17. Show IP protocols on router MEDELLIN2. Ingeniería de sistemas

MEDELLIN3

Se presenta la configuración de protocolo OSPF en el router MEDELLIN3 para mostrar el protocolo de información de enrutamiento como el vector de distancia, por medio de la configuración show IP protocolos para que los muestre. En la figura se muestra el encaminamiento de las interfaces en su versión 2 y sus direcciones.

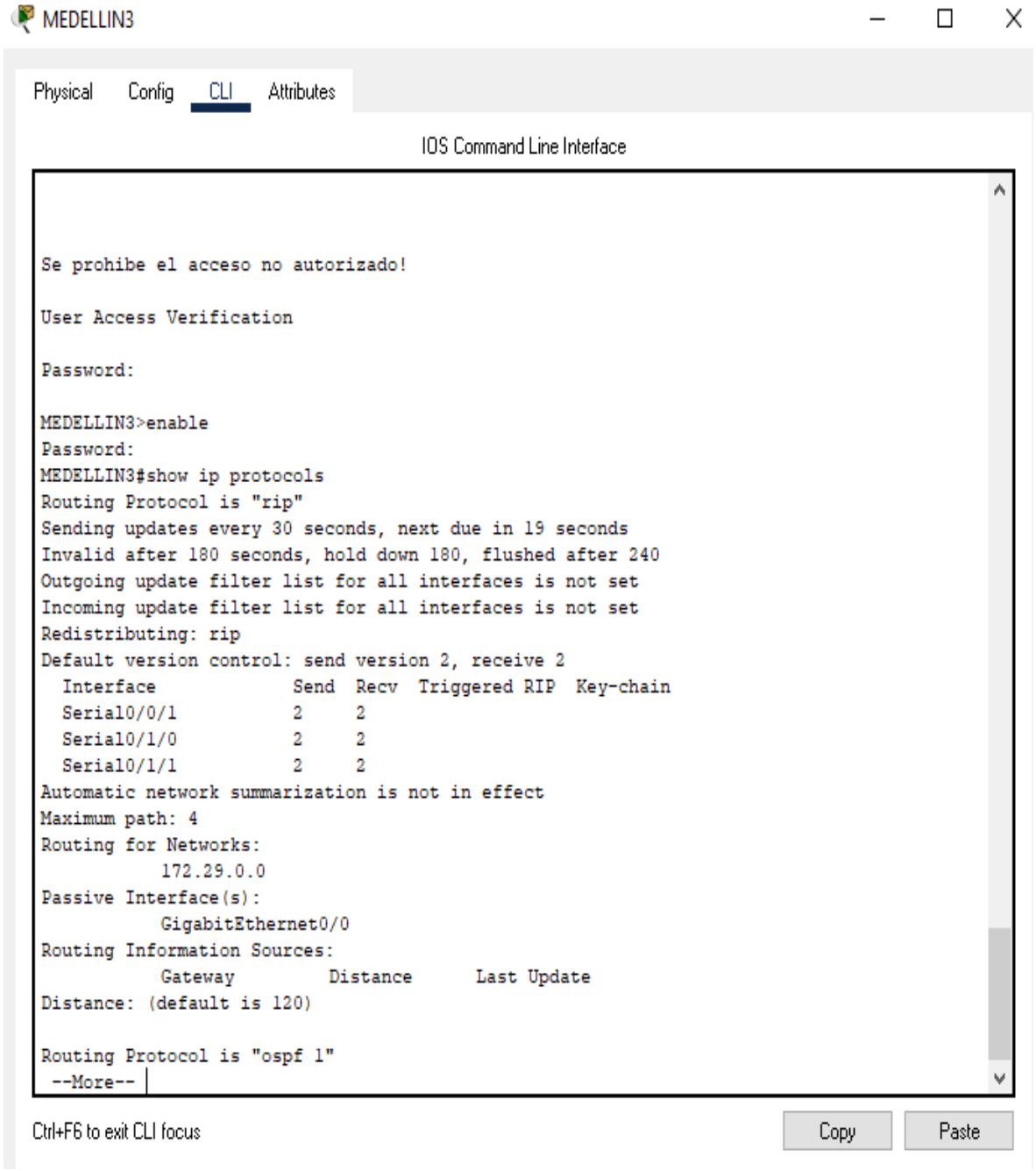


Figura 18. Show IP protocols on router MEDELLIN3. Ingeniería de sistemas

BOGOTA1

Se presenta la configuración de protocolo OSPF en el router MEDELLIN1 para mostrar el protocolo de información de enrutamiento como el vector de distancia, por medio de la configuración show IP protocolos para que los muestre. En la figura se muestra el encaminamiento de las interfaces en su versión 2 y sus direcciones.

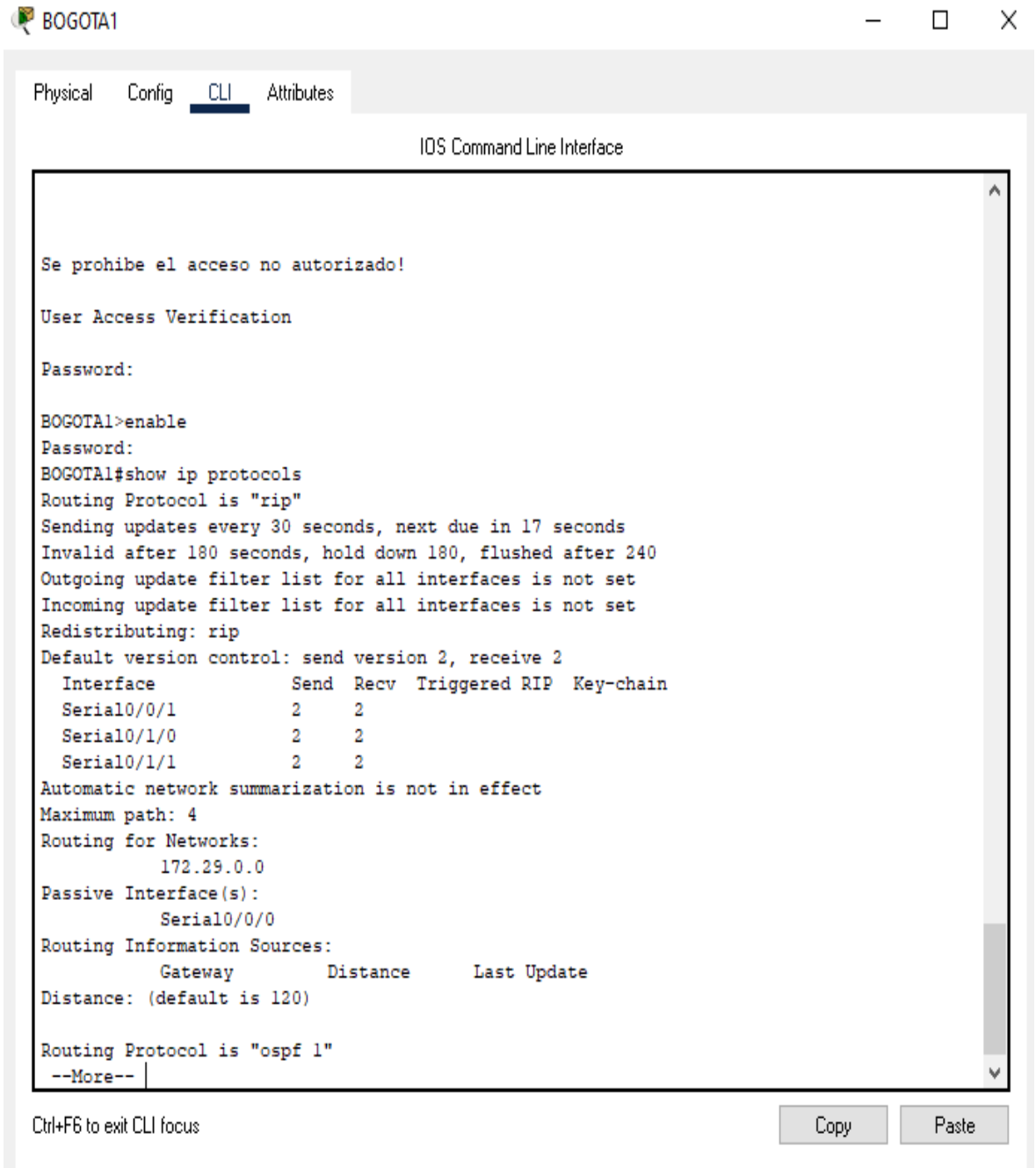


Figura 19. Show IP protocols on router BOGOTA1. Ingeniería de sistemas

BOGOTA2

Se presenta la configuración de protocolo OSPF en el router MEDELLIN1 para mostrar el protocolo de información de enrutamiento como el vector de distancia, por medio de la configuración show IP protocolos para que los muestre. En la figura se muestra el encaminamiento de las interfaces en su versión 2 y sus direcciones.

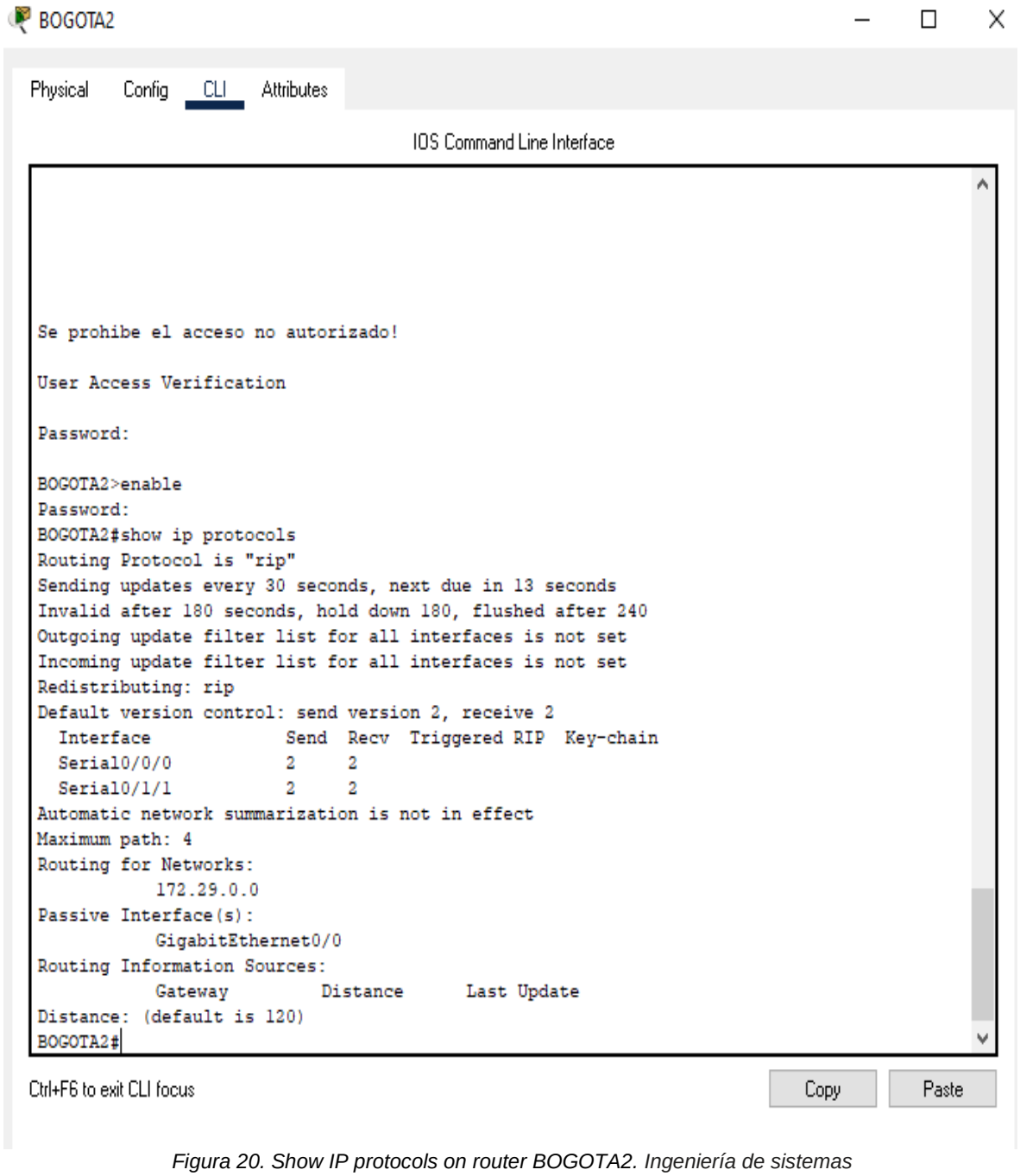


Figura 20. Show IP protocols on router BOGOTA2. Ingeniería de sistemas

BOGOTA3

Se presenta la configuración de protocolo OSPF en el router MEDELLIN1 para mostrar el protocolo de información de enrutamiento como el vector de distancia, por medio de la configuración show IP protocolos para que los muestre. En la figura se muestra el encaminamiento de las interfaces en su versión 2 y sus direcciones.

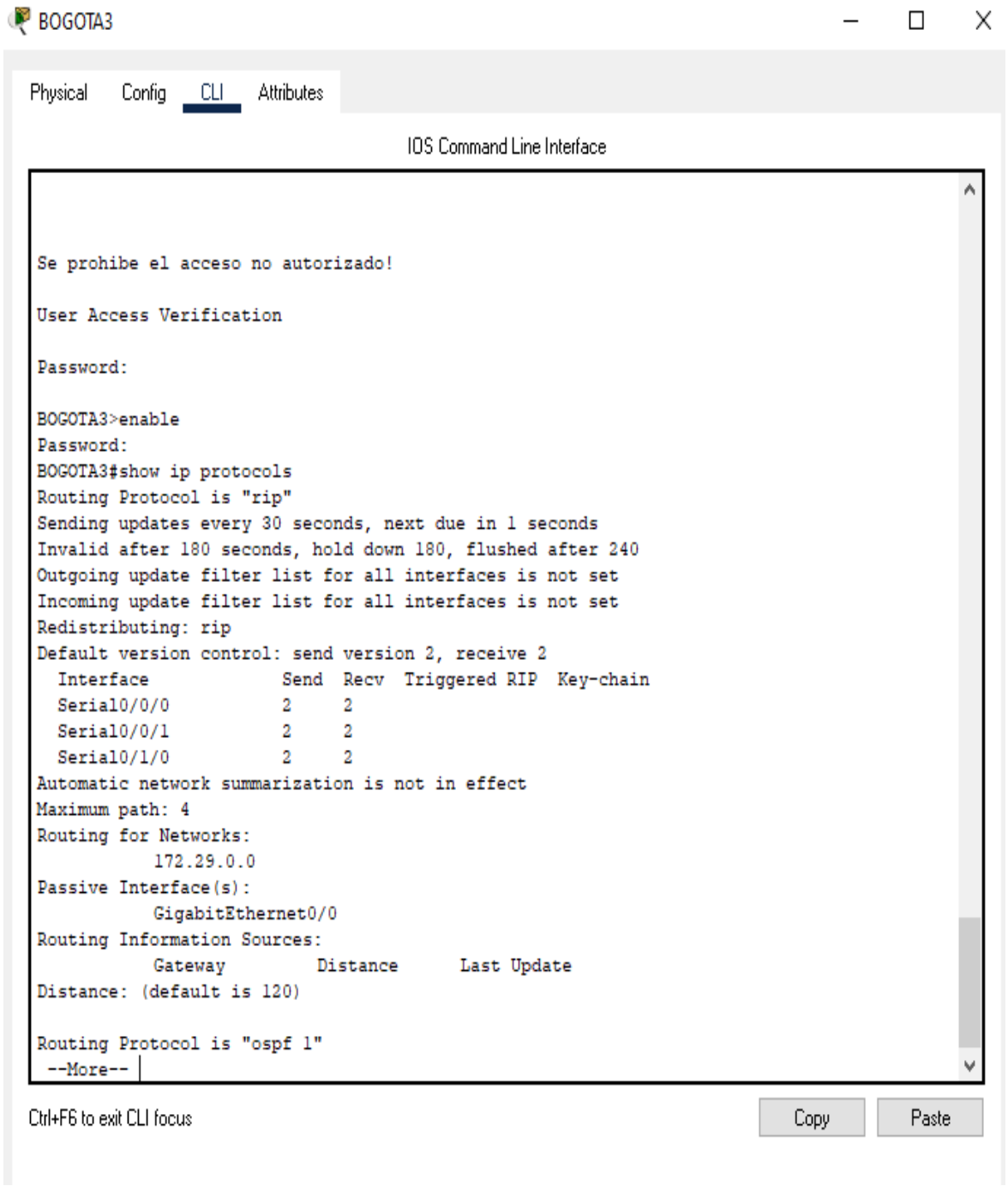


Figura 21. Show IP protocols on router BOGOTA3. Ingeniería de sistemas

b. Verificar y documentar la base de datos de OSPF de cada router, donde se informa de manera detallada de todas las rutas hacia cada red.

MEDELLIN1

Se presenta la configuración de protocolo OSPF en el router MEDELLIN1 para proporcionar un resumen de la información clave para todas las interfaces de red, por medio de la configuración show IP interface para que los muestre. En la figura se muestran la información claves de la interfase.

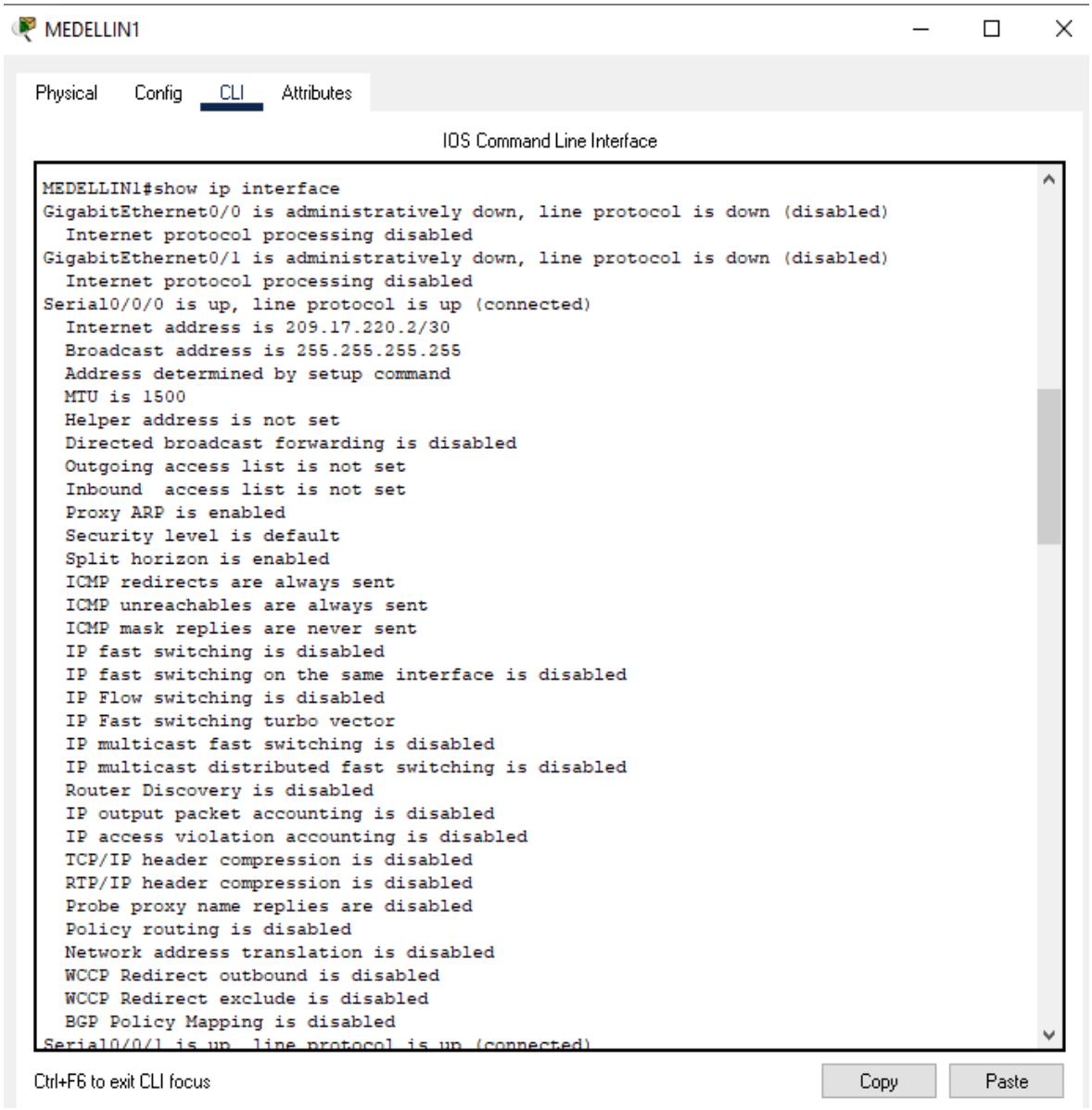


Figura 22. Show IP interface on router MEDELLIN1. Ingeniería de sistemas

MEDELLIN2

Se presenta la configuración de protocolo OSPF en el router MEDELLIN2 para proporcionar un resumen de la información clave para todas las interfaces de red, por medio de la configuración show IP interface para que los muestre. En la figura se muestran la información claves de la interfase.

Figura 23. Show IP interface on router MEDELLIN2. Ingeniería de sistemas

MEDELLIN3

Se presenta la configuración de protocolo OSPF en el router MEDELLIN3 para proporcionar un resumen de la información clave para todas las interfaces de red, por medio de la configuración show IP interface para que los muestre. En la figura se muestran la información claves de la interfase.

Figura 24. Show IP interface on router MEDELLIN3. Ingeniería de sistemas

BOGOTA1

Se presenta la configuración de protocolo OSPF en el router BOGOTA1 para proporcionar un resumen de la información clave para todas las interfaces de red, por medio de la configuración show IP interface para que los muestre. En la figura se muestran la información claves de la interfase.

Figura 25. Show IP interface on router BOGOTA1. Ingeniería de sistemas

BOGOTA2

Se presenta la configuración de protocolo OSPF en el router BOGOTA2 para proporcionar un resumen de la información clave para todas las interfaces de red, por medio de la configuración show IP interface para que los muestre. En la figura se muestran la información claves de la interfase.

Figura 26. Show IP interface on router BOGOTA2. Ingeniería de sistemas

BOGOTA3

Se presenta la configuración de protocolo OSPF en el router BOGOTA3 para proporcionar un resumen de la información clave para todas las interfaces de red, por medio de la configuración show IP interface para que los muestre. En la figura se muestran la información claves de la interfase.

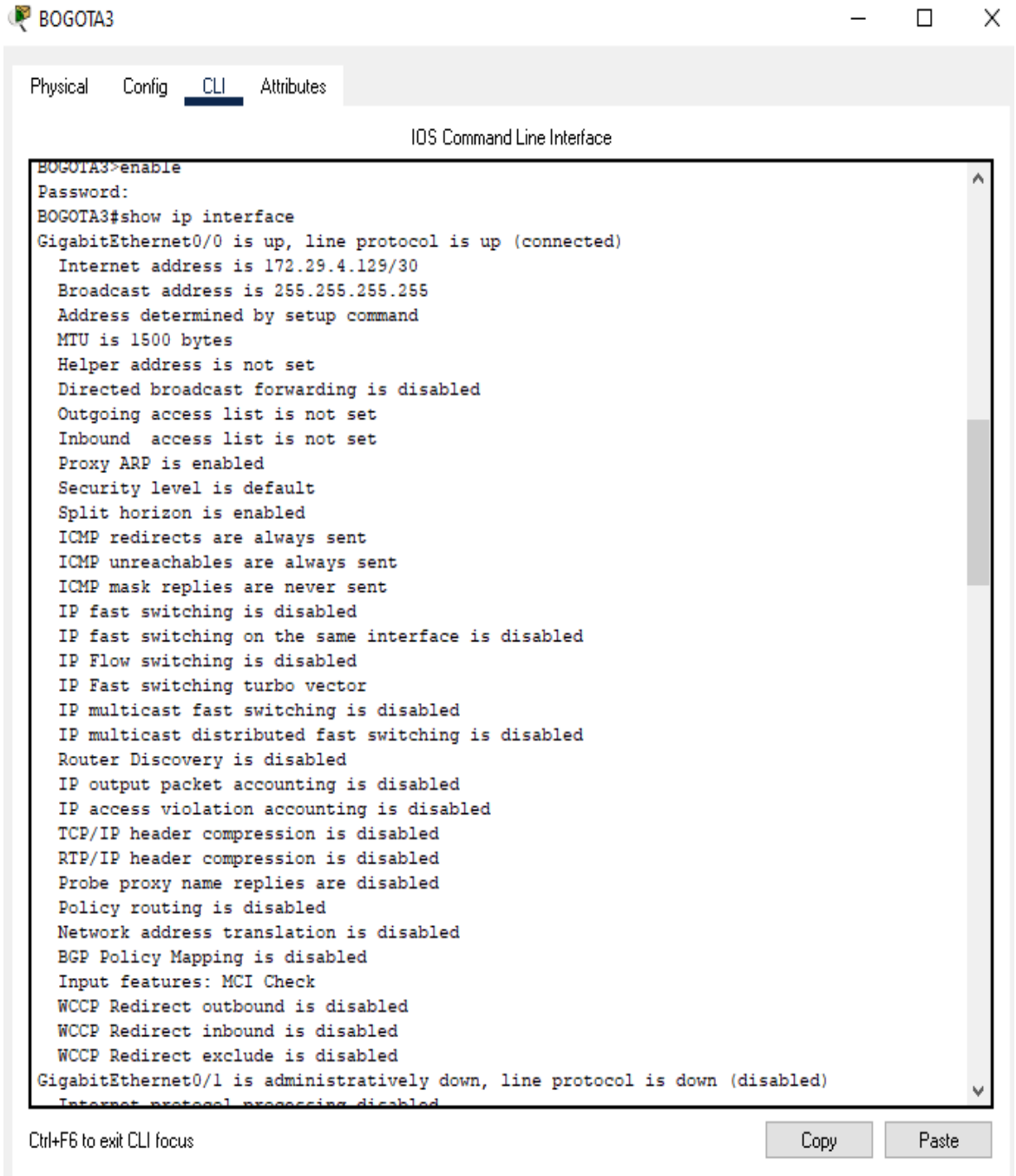


Figura 27. Show IP interface on router BOGOTA3. Ingeniería de sistemas

PARTE 5: Configurar encapsulamiento y autenticación PPP.

a. Según la topología se requiere que el enlace Medellín1 con ISP sea configurado con autenticación PAT.

ISP Int s0/0/1
encapsulation PPP
PPP authentication PAP
PPP PAP sent-username ISP password cisco

MEDELLIN1
interface serial 0/0/0
encapsulation PPP
PPP authentication PAP
PPP PAP sent-username MEDELLIN1 password cisco

b. El enlace Bogotá1 con ISP se debe configurar con autenticación CHAT

ISP
int s0/0/0
encapsulation PPP
PPP authentication PAP
PPP PAP sent-username ISP password cisco

BOGOTA1
int s0/0/0
encapsulation PPP
PPP authentication PAP
PPP PAP sent-username BOGOTA1 password cisco

PARTE 6: Configuración de PAT.

a. En la topología, si se activa NAT en cada equipo de salida (Bogotá1 y Medellín1), los routers internos de una ciudad no podrán llegar hasta los routers internos en el otro extremo, sólo existirá comunicación hasta los routers Bogotá1, ISP y Medellín1.

b. Después de verificar lo indicado en el paso anterior proceda a configurar el NAT en el router Medellín1. Compruebe que la traducción de direcciones indique las interfaces de entrada y de salida. Al realizar una prueba de ping, la dirección debe

ser traducida automáticamente a la dirección de la interfaz serial 0/1/0 del router Medellín1, cómo diferente puerto.

c. Proceda a configurar el NAT en el router Bogotá1. Compruebe que la traducción de direcciones indique las interfaces de entrada y de salida. Al realizar una prueba de ping, la dirección debe ser traducida automáticamente a la dirección de la interfaz serial 0/1/0 del router Bogotá1, cómo diferente puerto.

MEDELLIN1
ip access-list standard host
permit 172.29.4.0 0.0.0.255
exit
ip nat inside source list host interface serial 0/0/0 overload
int s0/0/0
ip nat outside
int s0/0/1
ip nat outside
int s0/1/0
ip nat outside
int s0/1/1
ip nat outside

BOGOTA1
ip access-list standard host
permit 172.29.0.0 0.0.0.255
exit
ip nat inside source list host interface serial 0/0/0 overload
int s0/0/0
ip nat outside
int s0/0/1
ip nat outside
int s0/1/0
ip nat outside
int s0/1/1
ip nat outside

PARTE 7: Configuración del servicio DHCP.
a. Configurar la red Medellín2 y Medellín3 donde el router Medellín 2 debe ser el servidor DHCP para ambas redes LAN.

MEDELLIN2
ip dhcp excluded-address 172.29.4.1 172.29.4.5
ip dhcp excluded-address 172.29.4.118 172.29.4.133
ip dhcp pool MEDELLIN2
etwork 172.29.4.0 255.255.255.128
default-router 172.29.4.1
dns-server 8.8.8.8
ip dhcp pool MEDELLIN3
network 172.29.4.128 255.255.255.128
default-router 172.29.4.129
dns-server 8.8.8.8

b. El router Medellín3 deberá habilitar el paso de los mensajes broadcast hacia la IP del router Medellín2.
MEDELLIN3
int s0/1/0
ip helper-addres 172.29.6.5

c. Configurar la red Bogotá2 y Bogotá3 donde el router Medellín2 debe ser el servidor DHCP para ambas redes LAN.
MEDELLIN2
ip dhcp excluded-address 172.29.0.1 172.29.0.4
ip dhcp excluded-address 172.29.1.1 172.29.1.4
ip dhcp pool BOGOTA2
network 172.29.1.0 255.255.255.0
default-router 172.29.1.1
dns-server 8.8.8.8
exitip dhcp pool BOGOTA3
network 172.29.0.0 255.255.255.0
default-router 172.29.0.1
dns-server 8.8.8.8

d. Configure el router Bogotá1 para que habilite el paso de los mensajes Broadcast hacia la IP del router Bogotá2.

BOGOTA1
int s0/0/1
ip helper-addres 172.29.3.13
exit

CONCLUSIONES

Por medio de las redes creadas se entendió como se puede conectar una empresa por medio de redes ya sea en diferentes ciudades o en una misma parte, se aprendió a programar claves y asegurar las redes para empezar. Saber cómo conectar las redes a los routers principales con sus respectivos nombres y claves de seguridad y a su vez conectar físicamente la topología de la red que incluye rutas estadísticas, protocolos OSPF y autenticación PPP y configuraciones PAT.

Estas configuraciones que se crean son para aprender a encaminar con un orden la pasarela interior al Gateway, por otro lado, también es importante saber el proceso que verifica al usuario de quien es, para una autenticación sencilla y por último, es importante configurar las PAT para conservar las direcciones del conjunto global interno al permitir que el router use las direcciones globales internas.

BIBLIOGRAFIA

- CISCO. (2017). Acceso a la red. Fundamentos de Networking. Recuperado de. https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#4.0.1.1
- CISCO. (2017). Asignación de direcciones IP. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module8/index.html#8.0.1.1
- CISCO. (2017). Capa de Aplicación. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module10/index.html#10.0.1.1
- CISCO. (2017). Capa de red. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#6.0.1.1
- CISCO. (2017). Capa de Transporte. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module7/index.html#7.0.1.1
- CISCO. (2017). Configuración y conceptos básicos de Switching. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module2/index.html#2.0.1.1
- CISCO. (2017). Configuración de un sistema operativo de red. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#2.0.1.1
- UNAD (2017). Configuración de Switches y Routers [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgL9QChD1m9EuGqC
- CISCO. (2017). Conceptos de Routing. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module4/index.html#4.0.1.1
- UNAD (2017). Diseño y configuración de redes con Packet Tracer [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgCT9VCtl_pLtPD9
- CISCO. (2017). DHCP. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module10/index.hml#10.0.1.1
- CISCO. (2017). Enrutamiento entre VLANs. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module5/index.html#5.0.1.1
- CISCO. (2017). Enrutamiento Estático. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module6/index.html#6.0.1.1

- CISCO. (2017). Enrutamiento Dinámico. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module7/index.html#7.0.1.1
- CISCO. (2017). Ethernet. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#5.0.1.1
- CISCO. (2017). Exploración de la red. Fundamentos de Networking. Recuperado de. https://static-course-assets.s3.amazonaws.com/ITN50ES/module1/index.html#1.0.1.1
- CISCO. (2017). Introducción a redes conmutadas. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module1/index.html#1.0.1.1
- CISCO. (2017). Listas de control de acceso. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module9/index.html#9.0.1.1
- CISCO. (2017). OSPF de una sola área. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module8/index.html#8.0.1.1
- CISCO. (2017). Protocolos y comunicaciones de red. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#3.0.1.1
- CISCO. (2017). Soluciones de Red. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module11/index.html#11.0.1.1
- CISCO. (2017). SubNetting. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module9/index.html#9.0.1.1
- CISCO. (2017). Traducción de direcciones IP para IPv4. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module11/index.html#11.0.1.1
- CISCO. (2017). VLANs. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module3/index.html#3.0.1.1
- Vesga, J. (2019). Introducción al Laboratorio Remoto SmartLab [OVI]. Recuperado de http://hdl.handle.net/10596/24167.
- UNAD (2017). PING y TRACER como estrategia en procesos de Networking [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei- NT1IhgTCtKY-7F5KIRC3
- UNAD (2017). Principios de Enrutamiento [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgOyjWeh6timi_Tm